(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 308 821 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.05.2003 Bulletin 2003/19

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **02019473.4**

(22) Date of filing: **30.08.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.10.2001 JP 2001332701**

(71) Applicant: **Hitachi, Ltd.**
Chiyoda-ku, Tokyo 101-8010 (JP)

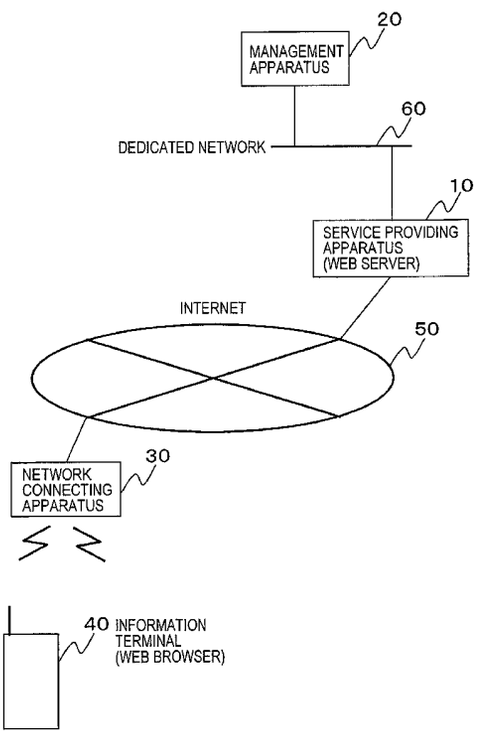
(72) Inventors:
- **Aoshima, Hirokazu, Hitachi, Ltd., Int. Prop. Group Chiyoda-ku, Tokyo 100-8220 (JP)**
- **Kaji, Tadashi, Hitachi, Ltd., Int. Prop. Group Chiyoda-ku, Tokyo 100-8220 (JP)**
- **Matsushima, Hitoshi, Hitachi,Ltd., Int.Prop.Group Chiyoda-ku, Tokyo 100-8220 (JP)**
- **Umezawa, Katsuyuki, Hitachi,Ltd., Int.Prop.Group Chiyoda-ku, Tokyo 100-8220 (JP)**
- **Yoshiura, Hiroshi, Hitachi,Ltd., Int.Prop.Group Chiyoda-ku, Tokyo 100-8220 (JP)**
- **Toyoshima, Hisashi, Hitachi,Ltd., Int.Prop.Group Chiyoda-ku, Tokyo 100-8220 (JP)**

(74) Representative: **Strehl Schübel-Hopf & Partner Maximilianstrasse 54 80538 München (DE)**

(54) System and method for authentication

(57) A system that can reduce possibility of outflow of private information in authentication of a user of an information terminal. A management apparatus has a user certificate DB in which a user certificate is registered in association with certificate identification information. Further, the management apparatus reads the user certificate associated with the certificate identification information sent from a service providing apparatus, from the user certificate DB, and judges whether the user certificate satisfies certain Web browsing conditions, to determine approval or denial of browsing the Web page concerned. Then, the management apparatus sends the service providing apparatus approval or denial information indicating the determination result. On the other hand, the service providing apparatus receives the certificate identification information from the information terminal, sends the certificate identification information to the management apparatus, and acquires the approval or denial information from the management apparatus. When the acquired approval or denial information indicates permission to browse the Web page, the service providing apparatus permits the information terminal to browse the Web page.

FIG.1



EP 1 308 821 A2

Description

BACKGROUND OF THE INVENTION

[0001] The present invention relates to a technique for authentication of, for example, a user of an information terminal.

[0002] Recently, has been proposed a system that utilizes a network such as the Internet for providing various services to a user of an information terminal. For example, systems that utilize a network for distributing contents or for executing various procedures such as electronic commerce have been proposed.

[0003] Sometimes, at the time of providing a service, a service provider requires a user of an information terminal to present his private information. Private information is required for confirming that the user of the information terminal satisfies service providing conditions (for example, age) for enjoying the service provided by the service provider. Thus, in the conventional systems, a service provider's apparatus receives private information from a user of an information terminal through a network, judges whether the private information satisfies predetermined service providing conditions, and determines whether the service is to be provided, based on the result of the judgment.

SUMMARY OF THE INVENTION

[0004] In the case of thus-described conventional systems that utilize a network for providing service, when a service provider requires a user of an information terminal to present his private information, the private information flows on the network, as described above. Further, it is possible to accumulate private information in the service provider's apparatus. This means that there is high possibility of outflow of the private information to a third party.

[0005] The present invention has been made taking the above-described circumstances into consideration, and reduces the possibility of outflow of private information at the time of authentication of an information terminal's user.

[0006] The authentication system of the present invention comprises a management apparatus that manages private information and a service providing apparatus that provides service to an information terminal.

[0007] The above-mentioned management apparatus comprises:

a private information database that registers private information (information for specifying a person including, for example, name, address, age, and existence of bank account), associating that private information with personal identification information (for example, personal ID number);

a providing condition database that registers service providing conditions (for example, age condition and existence of bank account) required for private information when the service providing apparatus provides the service;

a determination processing unit that reads private information associated with personal identification information (which is sent from the above-mentioned service providing apparatus) from the private information database; makes a judgment on whether the private information satisfies the service providing conditions registered in the providing condition database; and determines approval or denial of providing the service depending on a result of the judgment; and

a notification processing unit that notifies the service providing apparatus of approval or denial information indicating the judgment result of the determination processing unit.

[0008] Further, the above-mentioned service providing apparatus comprises:

a personal identification information acquisition processing unit that acquires personal identification information from the information terminal;

an approval or denial information acquisition processing unit that sends the personal identification information acquired by the personal identification information acquisition processing unit to the management apparatus, to acquire approval or denial information from the management apparatus; and

a service providing processing unit that provides the service to the information terminal, only when the approval or denial information acquired by the approval or denial information acquisition processing unit indicates permission to provide the service.

[0009] According to the present invention, owing to the above-described configuration, the information terminal sends personal identification information as identification information of private information, to the service providing apparatus. Further, the management apparatus sends approval or denial information, which indicates approval or denial of providing the service, to said service providing apparatus. Thus, possibility of outflow of private information itself can be reduced.

[0010] In the above-mentioned management apparatus, the private information database may register private information together with a public key certificate, associating the private information and the public key certificate with personal identification information. Further, the above-mentioned determination processing unit may verify digital signature information added to the personal identification information sent from the service providing apparatus, using a public key certificate registered in association with the personal identification information in said private information database; perform the judgment, only when the verification is successful;

determine approval or denial of providing the service depending on the result of the judgment; and, on the other hand, determine rejection of providing the service when the verification fails.

[0011] In that case, in the above-mentioned service providing apparatus, the personal identification information acquisition processing unit acquires the personal identification information added with the digital signature information, from the information terminal. And, the above-mentioned approval or denial information acquisition processing unit sends the management apparatus the personal identification information added with the digital signature information, which is acquired by the personal identification information acquisition processing unit, to acquire the approval or denial information from the said management apparatus.

[0012] Thus, it is possible to confirm that the user of the above-mentioned information terminal is a legitimate user specified by the private information corresponding to the personal identification information, by verifying the signature information that is generated by the information terminal and added to the personal identification information.

[0013] The authentication system of the present invention can be applied, for example, to a Web system in which browsing of a certain Web page is permitted only when private information satisfies predetermined service providing conditions. In that case, the above-mentioned information terminal functions as a Web browser, and the above-mentioned service providing apparatus functions as a Web server or as a network connecting apparatus that connects the information terminal to the Web server through a network.

[0014] Further, the authentication system of the present invention can be applied, for example, to a settlement system in which settlement required for purchasing a commodity or the like is permitted only when private information satisfies predetermined service providing conditions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]

Fig. 1 is a schematic diagram showing an authentication system to which a first embodiment of the present invention is applied;
Fig. 2 is a schematic diagram showing the service providing apparatus 10 shown in Fig. 1;
Fig. 3 is a schematic diagram showing the management apparatus 20 shown in Fig. 1;
Fig. 4 is a diagram showing an example of contents of registration in the user certificate DB 202 shown in Fig. 3;
Fig. 5 is a diagram showing an example of contents of registration in the service providing condition DB 203 shown in Fig. 3;
Fig. 6 is a schematic diagram showing the information terminal 40 shown in Fig. 1;
Fig. 7 is a diagram showing an example of a hardware configuration of the service providing apparatus 10 or the management apparatus 20 shown in Fig. 1;
Fig. 8 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 1;
Fig. 9 is a schematic diagram showing an authentication system to which a second embodiment of the present invention is applied;
Fig. 10 is a schematic diagram showing the service providing apparatus 30' shown in Fig. 9;
Fig. 11 is a diagram showing an example of contents of registration in the accounting DB 309 shown in Fig. 10;
Fig. 12 is a schematic diagram showing the management apparatus 20' shown in Fig. 9;
Fig. 13 is a diagram showing an example of contents of registration in the authentication mark DB 207 shown in Fig. 12;
Fig. 14 is a schematic diagram showing the information terminal 40' shown in Fig. 9;
Fig. 15 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 9;
Fig. 16 is a view showing an example of a Web page displayed together with a authentication mark on the information terminal 40';
Fig. 17 is a view showing an example of a Web page displayed together with a authentication mark on the information terminal 40';
Fig. 18 is a view showing an example of a Web page displayed together with a authentication mark on the information terminal 40';
Fig. 19 is a view showing an example of a Web page displayed together with a authentication mark on the information terminal 40';
Fig. 20 is a view showing an example of a Web page displayed together with a authentication mark on the information terminal 40';
Fig. 21 is a schematic diagram showing an authentication system to which a third embodiment of the present invention is applied;
Fig. 22 is a schematic diagram showing the service providing apparatus 70 shown in Fig. 21;
Fig. 23 is a diagram showing an example of contents of registration in the settlement DB 705 shown in Fig. 22;
Fig. 24 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 21; and
Fig. 25 is a diagram for explaining a variation of the operating procedure of the authentication system shown in Fig. 21.

DETAILED DESCRIPTION

[0016] Now, embodiments of the present invention will be described.

[0017] As a first embodiment of the present invention, will be taken an example in which the authentication system of the present invention is applied to a system that permits browsing of a certain Web page only to an information terminal (Web browser) of a user who satisfies predetermined service providing conditions.

[0018] Fig. 1 is a schematic diagram showing an authentication system to which the first embodiment of the present invention is applied.

[0019] In Fig. 1, a service providing apparatus 10 has a function of a Web server, and makes a Web page displayed on an information terminal 40 that has accessed the service providing apparatus 10 through the Internet 50. Further, the information terminal 40 is a radio terminal such as a portable telephone having a Web browser function, a PDA (Personal Digital Assistant), or the like. Identification information of a user certificate issued to the user of the information terminal 40 is registered in the information terminal 40. As the identification information, may be employed information that alone can hardly specify the private information of the user. For example, a public key certificate may be used as the identification information. Hereinafter, an identification information number is referred to as certificate identification information. Further, the user certificate is electronic data that describes private information (for example, information such as name, address, age, and existence of bank account) required for certifying the user, and issued by an issuer that has legitimate authority. Further, a network connecting apparatus 30 has functions of a radio base station and an ISP (Internet Service Provider), and offers service of connecting the information terminal 40 to the Internet 50. A management apparatus 20 gives certificate identification information to a user certificate to manage it. Further, the management apparatus 20 manages providing conditions (hereinafter, referred to as a Web page providing conditions) of each Web page provided by the service providing apparatus 10, associating the Web page providing condition with identification information (URL (Uniform Resource Locator) or information that can specify URL) of the Web page concerned (hereinafter, this identification information is referred to as Web page identification information). In Fig. 1, the management apparatus 20 is connected to the service providing apparatus 10 through a dedicated network 60. When, however, a communication technique (such as cipher communication or the like) that can ensure security is employed, the management apparatus 20 and the service providing apparatus 10 may be connected through the Internet 50.

[0020] In the above-described configuration, when there is a user's instruction, the information terminal 40 accesses a desired Web page held in the service providing apparatus 10, through the network connecting apparatus 30 and the Internet 50. At that time, if the Web page that the information terminal 40 is to browse is one whose Web page providing condition is managed by the management apparatus 20, then, the service providing apparatus 10 acquires the certificate identification information from the information terminal 40, and sends a verification request, which includes the certificate identification information and the Web page identification information of the Web page in question, to the management apparatus 20. Receiving the verification request, the management apparatus 20 specifies the user certificate managed in association with the certificate identification information included in that verification request, and specifies the Web page providing condition managed in association with the Web page identification information included in that verification request. Then, the management apparatus 20 judges whether the private information described in the specified user certificate satisfies the specified Web page providing condition, to determine approval or denial of providing the Web page, and sends approval or denial information, which indicates the content of the decision, to the service providing apparatus 10. Receiving the approval or denial information from the management apparatus 20, the service providing apparatus 10 makes the information terminal 40 display the Web page that the information terminal 40 desires to browse, in the case where the content of the approval or denial information indicates permission to provide the Web page. On the other hand, in the case where the content indicates rejection of providing the Web page, the service providing apparatus 10 makes the information terminal 40 display, for example, a Web page telling a message that browsing of the desired Web page is rejected, instead of the Web page that the information terminal 40 desires to browse.

[0021] Thus, in the present embodiment, the information terminal 40 sends certificate identification information, i.e., the identification information of a user certificate, to the service providing apparatus 10. Further, the management apparatus 20 sends approval or denial information, which indicates approval or denial of providing the Web page, to the service providing apparatus 10. In other words, the user certificate itself is not transmitted on the Internet 50 or the dedicated network 60. Accordingly, possibility of outflow of a user certificate or private information described in a user certificate to a third party can be reduced.

[0022] Next, components of the system shown in Fig. 1, i.e., the service providing apparatus 10, the management apparatus 20 and the information terminal 40 will be described. In the present embodiment, a conventional apparatus having functions of a radio base station and an ISP can be used as the network connecting apparatus 30. Thus, description of the network connecting apparatus 30 is omitted.

[0023] First, the service providing apparatus 10 will be described.

[0024] Fig. 2 is a schematic diagram showing the service providing apparatus 10.

[0025] In Fig. 2, an Internet IF unit 101 is an interface for communicating with the information terminal 40

through the Internet 50.

[0026] A dedicated network IF unit 102 is an interface for communicating with the management apparatus 20 through the dedicated network 60.

[0027] A Web page DB (database) 103 registers Web pages (HTML documents).

[0028] A Web page providing unit 104 manages correspondence between each Web page registered in the Web page DB 103 and its URL. Being accessed by the information terminal 40 through Internet IF unit 101, the Web page providing unit 104 reads the Web page corresponding to the URL of the destination of the access, from the Web page DB 103, and sends that Web page to the information terminal 40.

[0029] Further, the Web page providing unit 104 holds a Web management TBL (table) 1041. The Web management TBL 1041 registers Web page identification information of a Web page whose Web page providing condition is managed by the management apparatus 20, associating the Web page identification information with the URL of the Web page in question. However, in the case where Web page identification information is a URL, the Web management TBL 1041 registers Web page identification information of a Web page whose Web page providing condition is managed by the management apparatus 20. Being accessed by the information terminal 40 through the Internet IF unit 101, the Web page providing unit 104 examines whether the Web page identification information of the Web page corresponding to the URL of the destination of the access by the information terminal 40 is registered in the Web management TBL 1041, in order to judge whether permission of the management apparatus 20 is required to browse the Web page corresponding to the above-mentioned URL of the access destination.

[0030] A certificate identification information acquisition unit 105 acquires the certificate identification information (which is added with a signature by means of a signature key (for example, a secret key) of the user of the information terminal 40) from the information terminal 40, when the Web page providing unit 104 judges that permission of the management apparatus 20 is required to browse the Web page corresponding to the URL of the destination of the access by the information terminal 40 that has accessed the Web page providing unit 104 through the Internet IF unit 101.

[0031] When the Web page providing unit 104 judges that permission of the management apparatus 20 is required to browse the Web page corresponding to the URL of the destination of the access by the information terminal 40 that has accessed the Web page providing unit 104 through the Internet IF unit 101, an approval or denial information acquisition unit 106 acquires the Web page identification information of the Web page corresponding to the URL of the access destination, from the Web page providing unit 104, and acquires the certificate identification information, which is added with the signature by means of the signature key of the user of the information terminal 40, from the certificate identification information acquisition unit 105. Then, the approval or denial information acquisition unit 106 generates a verification request including the certificate identification information and the Web page identification information, and sends the verification request to the management apparatus 20 through the dedicated network IF unit 102. Then, receiving approval or denial information as an answer to the verification request, from the management apparatus 20, the approval or denial information acquisition unit 106 sends the received approval or denial information to the Web page providing unit 104.

[0032] When the Web page providing unit 104 receives the approval or denial information that indicates permission to browse the Web page, the Web page providing unit 104 reads the Web page corresponding to the above-mentioned URL of the access destination, from the Web page DB 103, and sends the Web page to the information terminal 40. On the other hand, when the approval or denial information indicates rejection of browsing the Web page, the Web page providing unit 104 reads a Web page corresponding to a predetermined URL (for example, a Web page telling a message that browsing of the desired Web page is rejected) from the Web page DB 103, to send it to the information terminal 40.

[0033] Next, the management apparatus 20 will be described.

[0034] Fig. 3 is a schematic diagram showing the management apparatus 20.

[0035] In Fig. 3, a dedicated network IF unit 201 is an interface for communicating with the service providing apparatus 10 through the dedicated network 60.

[0036] As shown in Fig. 4, a user certificate DB 202 registers private information (information representing person's attributes such as name, address, age, and existence of bank account) 2002 described in a user certificate and a verification key (for example, a public key certificate) 2023 for verifying a digital signature of a user, in association with certificate identification information 2021.

[0037] As shown in Fig. 5, a service providing condition DB 203 registers respective service providing conditions 2032 on the items constituting the private information, as conditions to be satisfied for browsing a Web page, in association with Web page identification information 2031.

[0038] An authentication unit 204 verifies a digital signature added to certificate identification information, using the verification key registered in the user certificate DB 202 being associated with the certificate identification information included in a verification request received from the service providing apparatus 10 through the dedicated network IF unit 201. When the verification of the digital signature is successful, then, the authentication unit 204 sends the certificate identification information included in the above-mentioned verification request and the Web page identification information to an

approval or denial judgment unit 205, to acquire a judgment result on approval of browsing the Web page from the approval or denial judgment unit 205. Then, the authentication unit 204 generates approval or denial information indicating the judgment result, and sends the approval or denial information to the service providing apparatus 10 that sent the above-mentioned verification request. When the verification of the signature fails, the authentication unit 204 generates approval or denial information indicating that browsing of the Web page is rejected, and sends the approval or denial information to the service providing apparatus 10 that sent the above-mentioned verification request.

[0039] The approval or denial judgment unit 205 reads the service providing conditions registered in association with the Web identification information received from the authentication unit 204, in the service providing condition DB 203, and reads the private information of the user certificate registered in association with the certificate identification information received together with that Web page identification information from the authentication unit 204, in the user certificate DB 202. Then, the approval or denial judgment unit 205 examines whether the read private information satisfies the read service providing conditions. When the service providing conditions are satisfied, the approval or denial judgment unit 205 judges that browsing of the Web page is to be permitted. On the other hand, when the service providing conditions are not satisfied, the approval or denial judgment unit 205 judges that browsing of the Web page is to be rejected. Then, the judgment result is sent to the authentication unit 204.

[0040] Next, the information terminal 40 will be described.

[0041] Fig. 6 is a schematic diagram showing the information terminal 40.

[0042] In Fig. 6, a radio communication unit 401 communicates wirelessly with the network connecting apparatus 30, and connects with the Internet 50 through the network connecting apparatus 30. An instruction receiving unit 402 comprises, for example, an operator panel, and receives input of various instructions and information from a user.

[0043] A Web page browsing unit 403 accesses the service providing apparatus 10 through the radio communication unit 401, acquires the Web page having a desired URL designated by the user through the instruction receiving unit 402, and displays the acquired Web page on a display unit 404 comprising, for example, a liquid crystal panel.

[0044] A storage unit 405 stores the certificate identification information and the signature key. Here, the storage unit 405 may be, for example, a memory card that can be inserted to and removed from the information terminal 40. In that case, suitably, the storage unit 405 may be provided from the issuer that issues a user certificate and a verification key. Or, the storage unit 405 may be a ROM directly mounted on a circuit board of the information terminal. In that case, suitably, a seller of the information terminal 40 may deliver the information terminal 40 to the user, in a state that the storage unit 405 stores the certificate identification information and the verification key.

[0045] According to an instruction received from the service providing apparatus 10 through the Web page browsing unit 403, a certificate identification information transmission unit 406 reads the certificate identification information and the verification key from the storage unit 405. Then, using the verification key, the certificate identification information transmission unit 406 generates a digital signature corresponding to the certificate identification information, and sends the certificate identification information added with the digital signature to the service providing apparatus 10.

[0046] Each of the service providing apparatus 10 and the management apparatus 20 having the above-described configurations may be implemented by a computer system of a common configuration such as shown in Fig. 7 for example, comprising a CPU 1001, a memory 1002, an external storage 1003 such as a hard disk unit, a reader 1007 for reading data from a portable storage medium 1009 such as a CD-ROM or DVD-ROM, an input unit 1005 such as a keyboard or mouse, an output unit 1006 such as a monitor, a communication unit 1004 for communicating with the Internet 50 or the dedicated network 60, and a bus 1008 connecting those component units. Or, each of the service providing apparatus 10 and the management apparatus 20 may be implemented by a network system comprising a plurality of such computer systems connected with one another through a network.

[0047] A program for realizing the above-mentioned service providing apparatus 10 or management apparatus 20 on such a computer system or network system may be loaded from an external storage 1003 or from a storage medium 1009 through the reader 1007 onto the memory 1002, to be executed by the CPU 1001. Or, such a program may be loaded from the Internet 50 or the dedicated network 60 through the communication unit 1004 onto the memory 1002, to be executed by the CPU 1001.

[0048] Further, the above-described information terminal 40 also may be implemented by a portable computer system, for example, having the hardware configuration of Fig. 7 without the reader 1007. In that case, an apparatus having a radio communication function, such as a portable telephone, may be used as the communication unit 1004. Further, a small-sized storage such as a ROM or a memory card may be used as the external storage 1003.

[0049] Next, operation of the authentication system having the above configuration will be described.

[0050] Fig. 8 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 1.

[0051] First, in the information terminal 40, when a browsing request including designation of a URL is re-

ceived from the user through the instruction receiving unit 402 (S1001), then, the Web browsing unit 403 accesses the service providing apparatus 10 through the radio communication unit 401 and the network connecting apparatus 30, to sends the above-mentioned browsing request (S1002).

[0052] In the service providing apparatus 10, when the browsing request is received from the information terminal 40 through the Internet IF unit 101, then, the Web page providing unit 104 confirms whether the URL included in the request is registered in the Web management TBL 1041 (S1003).

[0053] In the case where the URL included in the browsing request is not registered in the Web management TBL 1041, the Web page providing unit 104 reads the Web page corresponding to the above-mentioned URL from the Web page DB 103, and sends the Web page to the information terminal 40 through the Internet IF unit 101, so that the Web page browsing unit 403 of the information terminal 40 displays the Web page on the display unit 404. On the other hand, in the case where the URL included in the browsing request is registered in the Web management TBL 1041, the Web page providing unit 104 sends a message to that effect to the certificate identification information acquisition unit 105. Further, the Web page providing unit 104 sends the Web page identification information registered in association with the URL in the Web management TBL 1041 to the approval or denial information acquisition unit 106. Receiving the above-mentioned message, the certificate identification information acquisition unit 105 sends a certificate identification information transmission request to the information terminal 40 through the Internet IF unit 101 (S1004).

[0054] In the information terminal 40, when the Web page browsing unit 403 receives the certificate identification information transmission request from the service providing apparatus 10 through the radio communication unit 401, then, the Web page browsing unit 403 sends a message to that effect to the certificate identification information transmission unit 406. Receiving this message, the certificate identification information transmission unit 406 reads the certificate identification information and the signature key from the storage unit 405. Then, using the signature key, a digital signature to the certificate identification information is generated (S1005). Further, the certificate identification information transmission unit 406 adds the generated signature to the certificate identification information, to send them to the service providing apparatus 10 through the radio communication unit 401 (S1006).

[0055] Here, the transmissions and receptions for the certificate identification information communication between the service providing apparatus 10 and the information terminal 40 can be realized by utilizing Java (a trademark or registered trademark in USA and other countries, owned by Sun Microsystems, Inc., USA) or CGI (Common Gateway Interface), for example.

[0056] In the service providing apparatus 10, when the certificate identification information and signature are received from the information terminal 40 through the Internet IF 101, then, the certificate identification information acquisition unit 105 sends them to the approval or denial information acquisition unit 106. The approval or denial information acquisition unit 106 generates a verification request, which includes the certificate identification information and signature received from the certificate identification information acquisition unit 105 and the Web page identification information received from the Web page providing unit 104 in S1003, and sends the verification request to the management apparatus 20 through the dedicated network IF unit 102 (S1007).

[0057] In the management apparatus 20, when the verification request is received from the service providing apparatus 10 through the dedicated network IF unit 201, the authentication unit 204 reads the verification key registered in the user certificate DB 202 in association with the certificate identification information included in the verification request. Then, using the verification key, the authentication unit 204 verifies the signature to the certificate identification information, which is included in the verification request (S1008). When the verification of the signature is successful, then, the authentication unit 204 sends the certificate identification information and Web page identification information included in the verification request to the approval or denial judgment unit 205.

[0058] Receiving the certificate identification information and the Web page identification information, the approval or denial judgment unit 205 reads the user certificate registered in association with the certificate identification information in the user certificate DB 202, and reads the service providing conditions registered in association with the Web page identification information in the service providing condition DB 203. Then, the approval or denial judgment unit 205 examines whether the private information described in the user certificate satisfies the service providing conditions (for example, whether the age included in the private information satisfies the age condition prescribed in the service providing conditions). Then, the approval or denial judgment unit 205 sends the authentication unit 204 the judgment result to the effect that browsing of the Web page is permitted or rejected depending on whether the service providing conditions are or are not satisfied (S1009).

[0059] When the judgment result sent from the approval or denial judgment unit 205 indicates rejection of browsing the Web page, or when the verification of the signature fails in S1008, then, the authentication unit 204 generates approval or denial information to the effect that browsing of the Web page is rejected, and sends the approval or denial information to the service providing apparatus 10 through the dedicated network IF unit 201. On the other hand, when the judgment result sent from the approval or denial judgment unit 205 indi-

cates permission to browse the Web page, then, the authentication unit 204 generates approval or denial information to that effect, and sends the approval or denial information to the service providing apparatus 10 through the dedicated network IF unit 201 (S1010).

[0060] In the service providing apparatus 10, when the approval or denial information is acquired from the management apparatus 20 through the dedicated network IF unit 102, then, the approval or denial information acquisition unit 106 sends the approval or denial information to the Web page providing unit 104. When the approval or denial information received from the approval or denial information acquisition unit 106 indicates permission to browse the Web page, then, the Web page providing unit 104 reads the Web page corresponding to the URL included in the browsing request received in S1002, from the Web page DB 103, and sends the Web page to the information terminal 40 through the Internet IF unit 101, to make the Web page browsing unit 403 of the information terminal 40 display the Web page on the display unit 404. On the other hand, when the approval or denial information indicates rejection of browsing the Web page, the Web page providing unit 104 reads the Web page corresponding to the predetermined URL (for example, a Web page telling a message that browsing of the desired Web page is rejected) from the Web page DB 103, and sends the read Web page to the information terminal 40 through the Internet IF unit 101, to make the Web browsing unit 403 of the information terminal display this Web page on the display unit 404 (S1011).

[0061] Hereinabove, the first embodiment of the present invention has been described.

[0062] In the present embodiment, the information terminal 40 sends certificate identification information of a user certificate to the service providing apparatus 10. Further, the management apparatus 20 sends approval or denial information indicating approval or denial of browsing a Web page to the service providing apparatus 10. Thus, possibility of outflow of private information itself, which is described in a user certificate, can be reduced.

[0063] Further, in the present embodiment, the management apparatus 20 registers a user certificate together with the verification key (for example, a public key certificate) of the signature, associating them with the certificate identification information, in the user certificate DB 202. And, the authentication unit 204 verifies a digital signature to certificate identification information included in a verification request sent from the service providing apparatus 10, using the verification key registered in association with the certificate identification information in the user certificate DB 202. By this arrangement, it is possible to confirm that the user of the information terminal 40 is a legitimate user who can be specified by the user certificate corresponding to the certificate identification information.

[0064] In the above-described embodiment, the service providing apparatus 10 may be provided with an authentication unit for verification of a signature, so that verification of a signature added to certificate identification information is performed in the service providing apparatus 10 instead of the authentication unit 204 of the management apparatus 20. In that case, the service providing apparatus 10 may acquire the verification key together with the certificate identification information and the signature to the certificate identification information, from the information terminal 40.

[0065] Further, in the above-described embodiment, the service providing apparatus 10 may be provided with an approval or denial judgment unit so that the judgment on approval or denial of browsing a Web page is made in the service providing apparatus 10 instead of the approval or denial judgment unit 205 of the management apparatus 20. In that case, the service providing condition DB 203 of the management apparatus 20 registers private information items required for judgment of approval or denial of browsing a Web page, in association with the Web page identification information concerned. The service providing apparatus 10 is made to send an information transmission request including certificate identification information and Web page identification information, to the management apparatus 20. Then with respect to the private information items registered in the service providing condition DB 203 in association with the Web page identification information included in the above-mentioned information transmission request, the management apparatus 20 extracts those private information items from the user certificate registered in the user certificate DB 202 in association with the certificate identification information included in the above-mentioned information transmission request, and sends the extracted private information items to the service providing apparatus 10. In this case also, possibility of outflow of private information can be reduced in comparison with the conventional case, since the private information sent to the service providing apparatus 10 is limited to the private information items whose transmission is permitted by the management apparatus 20 (i.e., information items actually required for judgment on Web page browsing).

[0066] Further, in the above-described embodiment, the certificate identification information acquisition unit 105 of the service providing apparatus 10 may have the following function. Namely, prior to acquisition of certificate identification information from an information terminal 40, the certificate identification information acquisition unit 105 displays a message asking whether transmission of the certificate identification information is agreed, on the display unit 404 of the information terminal 40. And, only when the user of the information terminal 40 agrees, the certificate identification information is acquired from the information terminal 40.

[0067] Next, a second embodiment of the present invention will be described.

[0068] As the second embodiment of the present in-

vention, will be taken an example in which the authentication system of the present invention is applied to a system in which a service providing apparatus (a network connecting apparatus) permits access to a certain Web page opened by a Web server, only to an information terminal (a Web browser) of a user who satisfies predetermined service conditions.

[0069] Fig. 9 is a schematic diagram showing an authentication system to which the second embodiment of the present invention is applied. In this figure and Fig. 1 showing the first embodiment, same reference numerals refer to elements having same functions.

[0070] In Fig. 9, a Web server 10' makes an information terminal 40' display a Web page, when the information terminal 40' accesses the Web server 10' through the Internet 50. Here, in the Web server 10', a Web page used for moving to a Web page to which Web page providing conditions are set includes an authentication mark that has been issued to the above-mentioned Web page to which the Web page providing conditions are set, or to a person concerned such as a sender or author of that Web page. The authentication mark is electronic image data in which Web page attribute information and a signature to the Web page attribute information are embedded utilizing the electronic watermark technique or the like. Here, the Web page attribute information is, for example, Web page identification information (such as URL) and other relevant information required for certifying a Web page. An authentication mark is issued by an issuer that has legitimate authority. Further, a service providing apparatus 30' has a function as a network connecting apparatus, or, in detail, functions as a radio base station and an ISP, and offers service of connecting the information terminal 40' to the Internet 50. And, a management apparatus 20' gives certificate identification information to a user certificate to manage it, and manages Web page identification information of a Web page certified by a authentication mark, associating the Web page identification information with the Web page providing conditions of the Web page in question and the Web page identification information (referred to as related Web page identification information) of the Web page that includes the authentication mark in question.

[0071] In Fig. 9, the management apparatus 20' is connected to the service providing apparatus 30' through a dedicated network 60. However, the management apparatus 20' and the service providing apparatus 30' may be connected through the Internet 50, when a communication technique (such as cipher communication or the like) that can ensure security is employed.

[0072] In the above-described configuration, when there is a user's instruction, the information terminal 40' accesses the Web server 10' through the network connecting apparatus 30' and the Internet 50, to display a desired Web page. At that time, if the displayed Web page includes a authentication mark, the user of the information terminal 40' can use the authentication mark in order to access the Web page certified by the authentication mark, and/or in order to acquire information on relation between the above-mentioned displayed Web page (Web page added with the authentication mark) and the Web page certified by the above-mentioned authentication mark.

[0073] When the Web page that the information terminal 40' is to browse is a Web page whose Web page providing conditions are managed by the management apparatus 20', namely, the Web page certified by the authentication mark, then, the service providing apparatus 30' acquires the certificate identification information from the information terminal 40', and sends a verification request, which includes the certificate identification information and the Web page identification information of the Web page in question, to the management apparatus 20'. Receiving the verification request, the management apparatus 20' specifies the user certificate managed in association with the certificate identification information included in the verification request, and specifies the Web page providing conditions managed in association with the Web page identification information included in the verification request. Then, the management apparatus 20' judges whether the private information described in the specified user certificate satisfies the above-mentioned specified Web page providing conditions, to determine approval or denial of providing the Web page, and sends approval or denial information that indicates the content of the determination to the service providing apparatus 30'. Receiving the approval or denial information from the management apparatus 20', the service providing apparatus 30' permits the information terminal 40' to access the Web page that the information terminal 40 desires to browse, when the content of the determination indicates permission to provide the Web page. On the other hand, when the content of the determination indicates rejection of providing the Web page, the service providing apparatus 30' makes the information terminal 40' display, for example, a Web page including a message that access to the desired Web page is rejected, instead of the Web page that the information terminal 40' desires to browse.

[0074] Further, when the service providing apparatus 30' receives a relation verification request, which includes Web page attribution information and related Web page identification information, from the information terminal 40', the service providing apparatus 30' sends the relation verification request to the management apparatus 20'. Receiving the relation verification request, the management apparatus 20' examines whether the Web page identification information of the Web page specified by the Web page attribute information included in the relation verification request is managed in association with the related Web page identification information included in the relation verification request. Then, the management apparatus 20' sends the result (referred to as relation verification result) to the service providing apparatus 30'. Based on the relation verification result received from the management appa-

ratus 20', the service providing apparatus 30' makes the information terminal 40' display a message on the relation between the Web page displayed by the information terminal 40' and the Web page certified by the above-mentioned authentication mark.

[0075] Thus, in the present embodiment, the information terminal 40' sends the service providing apparatus 30' certificate identification information of a user certificate. Further, the management apparatus 20' sends the service providing apparatus 30' approval or denial information that indicates approval or denial of providing a Web page. In other words, a user certificate itself is not transmitted on the Internet 50 or the dedicated network 60. Accordingly, possibility of outflow of a user certificate or private information described in a user certificate to a third party can be reduced.

[0076] Further, in the present embodiment, the user of the information terminal 40' can use a authentication mark added to a Web page to confirm a relation between the Web page in question and a Web page certified by the above-mentioned authentication mark. Thus, from the viewpoint of the user of the information terminal 40', security of using a Web is improved.

[0077] Next, components of the system shown in Fig. 9, i.e., the service providing apparatus 30', the management apparatus 20' and the information terminal 40' will be described. In the present embodiment, a conventional Web server can be used as the Web server 10'. And, thus, description of the Web server 10' is omitted.

[0078] First, the service providing apparatus 30' will be described.

[0079] Fig. 10 is a schematic diagram showing the service providing apparatus 30'.

[0080] In Fig. 10, a radio IF unit 301 is an interface for communicating with the information terminal 40' by radio communication.

[0081] An internet IF unit 302 is an interface for communicating with the Web server 10' through the Internet 50.

[0082] A dedicated network IF unit 303 is an interface for communicating with the management apparatus 20' through the dedicated network 60.

[0083] A repeater unit 304 connects the radio IF unit 301 and the Internet IF unit 302 to relay communication between the Web server 10' and the information terminal 40'.

[0084] Further, the repeater unit 304 holds a Web management TBL 3041. The Web management TBL 3041 registers Web page identification information of a Web page whose Web page providing conditions are managed by the management apparatus 20', associating the Web page identification information with the URL of the Web page in question. However, in the case where Web page identification information is a URL, the Web management TBL 3041 registers Web page identification information of a Web page whose Web page providing conditions are managed by the management apparatus 20'. The repeater unit 304 examines whether the Web page identification of the Web page corresponding to the URL of the destination of the access by the information terminal 40', which is in communication with the radio IF unit 301, is registered in the Web management TBL 3041, in order to judge whether permission of the management apparatus 20' is required to access the Web page corresponding to the above-mentioned URL of the access destination.

[0085] A certificate identification information acquisition unit 305 acquires the certificate identification information added with a signature by means of a signature key (for example, a secret key) of the user of the information terminal 40', from the information terminal 40', when the repeater unit 304 judges that permission of the management apparatus 20' is required to access the Web page corresponding to the URL of the destination of the access by the information terminal 40' in communication with the radio IF unit 301.

[0086] When the repeater unit 304 judges that permission of the management apparatus 20' is required to access the Web page corresponding to the URL of the destination of the access by the information terminal 40' that is in communication with the radio IF unit 301, then, an approval or denial information acquisition unit 306 acquires the Web page identification information of the Web page corresponding to the above-mentioned URL of the access destination, from the repeater unit 304, and acquires the certificate identification information added with the signature by means of the signature key of the user of the information terminal 40', from the certificate identification information acquisition unit 305. Then, the approval or denial information acquisition unit 306 generates verification request including the Web page identification information and the certificate identification information, and sends the verification request to the management apparatus 20' through the dedicated network IF unit 303. Then, receiving approval or denial information as an answer to the verification request, from the management apparatus 20', the approval or denial information acquisition unit 306 sends the received approval or denial information to the repeater unit 304.

[0087] When the repeater unit 304 receives the approval or denial information that indicates permission to access the Web page, the repeater unit 304 relays communication between the Web server 10' and the information terminal 40', to permit access to the Web page corresponding to the above-mentioned URL of the access destination. On the other hand, when the approval or denial information indicates rejection of accessing the Web page, the repeater unit 304 does not relays communication between the Web server 10' and the information terminal 40', and sends the information terminal 40' a predetermined Web page (for example, a Web page describing a message that browsing of the desired Web page is rejected) in the management apparatus 30'.

[0088] A relation information acquisition unit 307 sends the relation verification request, which is received

from the information terminal 40' through the radio IF unit 301, to the management apparatus 20' through the dedicated network IF unit 303. Then, the relation information acquisition unit 307 receives from the management apparatus 20' a relation verification result, which includes the verification result on a relation between the Web page displayed by the information terminal 40' (the Web page added with the authentication mark) and the Web page certified by the authentication mark, and sends the information terminal 40' a message on the above-mentioned relation, based on this relation verification result.

[0089] As shown in Fig. 11, for each Web page identification information 3091 of a Web page managed in the Web management TBL 3041, an accounting DB 309 registers certificate identification information 3092 of a user of an information terminal 40' who has used the Web page and the frequency 3093 of using the Web page, in association with the Web page identification information 3091 in question. The registration contents of the accounting DB 309 are used as accounting information for calculating charges to a user of an information terminal 40' for using Web pages (Web pages managed by the Web management TBL 3041).

[0090] When the repeater unit 304 permits the information terminal 40' to access a Web page whose Web page identification information is managed by the Web management TBL 3041, then, an accounting unit 308 adds 1 to the frequency of using the Web page that is associated with the above-mentioned Web page identification information and the certificate identification information of the user of the information terminal 40' in the accounting DB 309. Or, the accounting unit 308 registers anew the certificate identification information of the user and the use frequency "1", in association with the above-mentioned Web page identification information, in the accounting DB 309.

[0091] Next, the management apparatus 20' will be described.

[0092] Fig. 12 is a schematic view showing the management apparatus 20'. In this figure and Fig. 3 showing the management apparatus 20, same reference numerals refer to elements having same functions.

[0093] As shown in Fig. 13, for each Web page identification information 2071 of a Web page certified by an authentication mark, an authentication mark DB 207 shown in Fig. 12 registers related Web page identification information 2072, as Web page identification information of a Web page displayed together with the authentication mark, and the verification key (for example, a public key certificate) 2073 for verifying a signature of the authentication mark issuer.

[0094] Using a verification key registered in the authentication mark DB 207 in association with Web page identification information included in a relation verification request received from the service providing apparatus 30' through the dedicated network IF unit 201, a relation verification unit 206 verifies the signature added to the Web page identification information. When the verification of the signature is successful, then, the relation verification unit 206 examines whether the related Web page identification information registered in the authentication mark DB 207 in association with the Web identification information included in the above-mentioned relation verification request coincides with the related Web identification information included in the above-mentioned relation verification request. Then, the relation verification unit 206 generates a relation verification result including the results of the above-mentioned verification of the signature and the verification of the coincidence), and sends the relation verification result to the service providing apparatus 30' that has sent the verification request.

[0095] Next, the information terminal 40' will be described.

[0096] Fig. 14 is a schematic diagram showing the information terminal 40'. In this figure and Fig. 6 showing the information terminal 40, same reference numerals refer to elements having same functions.

[0097] In Fig. 14, an authentication mark verification requesting unit 407 monitors a user's instruction inputted to a Web page displayed by the Web page browsing unit 403 and to an instruction receiving unit 402, in order to detect an action of selecting the authentication mark displayed in the Web page of the user. This can be realized, for example, by predetermining a name or a file extension of image data expressing an authentication mark, and by examining whether a name or a file extension of data that is specified in an HTML document to be displayed at the location selected by a user by means of a pointing device or the like is the above-mentioned name or the file extension predetermined.

[0098] When the above-mentioned action of selecting is detected, then, for example as shown in Fig. 17, the authentication mark verification requesting unit 407 displays a menu for receiving an instruction of a user, such as an instruction of a relation verification request or an instruction of a browsing request for the Web page certified by the authentication mark, using a balloon display or the like. When an instruction of a relation verification request is received from the user through the menu, then, the authentication mark verification requesting unit 407 extracts the Web page identification information and the signature of the authentication mark issuer, which are embedded in the authentication mark utilizing the electronic watermark technique or the like. Then, the authentication mark verification requesting unit 407 generates a relation verification request, which includes the extracted identification information and signature and the URL of the Web page displayed now by the Web page browsing unit 403, and sends the generated request to the service providing apparatus 30' through the radio communication unit 401. On the other hand, when an instruction of a browsing request is received, the authentication mark verification requesting unit 407 extracts the Web page identification information embed-

ded in the authentication mark, using the electronic watermark technique or the like, generates a browsing request including the URL specified by the extracted Web page identification information, and sends the request to the service providing apparatus 30' through the radio communication unit 401.

[0099] Similarly to the management apparatus 20 etc. of the first embodiment, also each of the service providing apparatus 30' and the management apparatus 20' having the above-described configurations may be implemented, for example, by the computer system having the configuration shown in Fig. 7, or by a network system comprising a plurality of such computer systems connected one another through a network.

[0100] Similarly, also the above-described information terminal 40' may be implemented by a portable computer system, for example, having the hardware configuration of Fig. 7 without the reader 1007. In that case, an apparatus having a radio communication function, such as a portable telephone, may be used as the communication unit 1004. Further, a small-sized storage such as a ROM or a memory card may be used as the external storage 1003.

[0101] Next, operation of the authentication system having the above configuration will be described.

[0102] Fig. 15 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 9.

[0103] In the service providing apparatus 30', when a Web page browsing request including designation of a URL is received from the information terminal 40' through the radio communication IF unit 301, the repeater unit 304 confirms whether this URL is registered in the Web management TBL 3041. In the case where the URL is not registered, the repeater unit 304 sends the browsing request to the Web server 10' through the Internet IF unit 302. Receiving this, the Web server 10' sends the Web page corresponding to the URL included in the above-mentioned browsing request, to the information terminal 40' through the service providing apparatus 30'. The information terminal 40' displays the Web page received from the Web server 10' through the service providing apparatus 30'. At that time, when the Web page includes an authentication mark, this authentication mark is displayed additionally (S2001).

[0104] Fig. 16 shows an example of a Web page including an authentication mark. As described above, the authentication mark 1601 is embedded with the Web page identification information of the Web page certified by the authentication mark and the signature of the authentication mark issuer to the Web page identification information.

[0105] In the information terminal 40', when the authentication mark verification requesting unit 407 detects that the authentication mark 1601 on the Web page displayed by the Web page browsing 403 is selected by the user through the instruction receiving unit 402, then, the authentication mark verification requesting unit 407 displays a balloon menu 1602 as shown in Fig. 17 on the Web page. Here, the balloon menu includes items for receiving instructions such as an instruction 1603 of a relation verification request and an instruction 1604 of a Web page browsing request.

[0106] When, in the screen shown in Fig. 17, the authentication mark verification requesting unit 407 detects that the user selects the instruction 1603 of the relation verification request through the instruction receiving unit 402 (S2002), then, the authentication mark verification requesting unit 407 extracts the Web page identification information and the signature to the Web page identification information embedded in the authentication mark 1601, utilizing the electronic watermark technique, or the like. Further, the authentication mark verification requesting unit 407 generates a relation verification request, which includes the extracted information and the related Web page identification information specified from the URL of the Web page displayed now, or the like, and sends the generated relation verification request to the service providing apparatus 30' through the radio communication unit 401 (S2003).

[0107] In the service providing apparatus 30', the relation information acquisition unit 307 sends the relation verification request, which is received from the information terminal 40' through the radio IF unit 301, to the management apparatus 20' through the dedicated network IF unit 303 (S2004).

[0108] In the management apparatus 20', receiving the relation verification request from the service providing apparatus 30' through the dedicated network IF unit 303, the relation verification unit 206 reads the verification key registered in the authentication mark DB 207 in association with the Web page identification information included in the relation verification request. Then, using the verification key, the relation verification unit 206 verifies the signature added to the Web page identification information (S2005).

[0109] When the verification of the signature is successful, the relation verification unit 206 verifies whether the related Web page identification information registered in the authentication mark DB 207 in association with the Web page identification information included in the relation verification request coincides with the related Web page identification information included in the relation verification request (S2006).

[0110] Then, the relation verification unit 206 generates a relation verification result, which includes the results of the verification of the signature and the verification of the coincidence, and sends the relation verification result to the service providing apparatus 30' through the dedicated network IF unit 201 (S2007).

[0111] In the service providing apparatus 30', receiving the relation verification result from the management apparatus 20' through the dedicated network IF unit 303, the relation information acquisition unit 307 sends a message corresponding to the contents of the relation verification result to the information terminal 40' through the IF unit 301 (S2008).

[0112] In response, the authentication mark verification requesting unit 407 of the information terminal 40' displays the message 1605 received from the service providing apparatus 30' through the radio communication unit 401, on the Web page, as shown in Figs. 18 - 20. Here, Fig. 18 shows an example for the case where the signature verification in S2005 fails. In this case, there is a possibility that the authentication mark is generated illegally by a third party other than the authentication mark issuer. Fig. 19 shows an example for the case where the signature verification in S2005 is successful but the coincidence verification in S2006 fails. In this case, there is a high possibility that the authentication mark issued by the authentication mark issuer is used illegally by a third party who does not have a legitimate right of using. And, Fig. 20 shows an example for the case where both the signature verification in S2005 and coincidence verification in S2006 are successful. In this case, there is a strong possibility that the authentication mark issued by the authentication mark issuer is used by a person who has a legitimate right of using the authentication mark.

[0113] On the other hand, in the screen shown in Fig. 17, when the authentication mark verification requesting unit 407 detects that the user selects the instruction 1604 of the browsing request through the instruction receiving unit 402 (S2009), then, the authentication mark verification requesting unit 407 extracts the Web page identification information embedded in the authentication mark 1601, utilizing the electronic watermark technique, or the like. Then, the authentication mark verification requesting unit 407 generates a browsing request including the URL specified by the Web page identification information, and sends the browsing request to the service providing apparatus 30' through the radio communication unit 401 (S2010).

[0114] In the service providing apparatus 30', receiving the Web page browsing request including the designation of the URL from the information terminal 40' through the radio IF unit 301, the repeater unit 304 confirms whether the URL is registered in the Web management TBL 3041 (S2011). When it is registered, the repeater unit 304 sends a message to that effect to the certificate identification information acquisition unit 305. Further, the repeater unit 304 sends the Web page identification information registered in association with the URL in the Web management TBL 3041 to the approval or denial information acquisition unit 306. Receiving the message, the certificate identification information acquisition unit 305 sends a certificate identification information transmission request to the information terminal 40' through the radio IF unit 301 (S2012).

[0115] In the information terminal 40', receiving the certificate identification information transmission request from the service providing apparatus 30' through the radio communication unit 401, the Web browsing unit 403 sends a message to that effect to the certificate identification information transmission unit 406. Receiving the message, the certificate identification information transmission unit 406 reads the certificate identification information and the verification key from the storage unit 405, and generates a digital signature to the certificate identification information, using the verification key (S2013). Then, the certificate identification information transmission unit 406 sends the certificate identification information added with the generated signature, to the service providing apparatus 30' through the radio communication unit 401 (S2014).

[0116] In the service providing apparatus 30', receiving the certificate identification information and the signature from the information terminal 40' through the radio IF unit 301, the certificate identification information acquisition unit 305 sends them to the approval or denial information acquisition unit 306. The approval or denial information acquisition unit 306 generates a verification request including the certificate identification information and signature received from the certificate identification information acquisition unit 305 and the Web page identification information received in S2011 from the repeater unit 304, and sends the verification request to the management apparatus 20' through the dedicated network IF unit 303 (S2015).

[0117] In the management apparatus 20', receiving the verification request from the service providing apparatus 30' through the dedicated network IF unit 201, the authentication unit 204 reads the verification key registered in the user certificate DB 202 in association with the certificate identification information included in the verification request. Then, using the verification key, the authentication unit 204 verifies the signature to the certificate identification information, which is included in the verification request (S2016). When the verification of the signature is successful, the authentication unit 204 sends the approval or denial judgment unit 205 the certificate identification information and Web page identification information included in the verification request.

[0118] Receiving them, the approval or denial judgment unit 205 reads the user certificate registered in association with the certificate identification information in the user certificate DB 202, and reads the service providing conditions registered in association with the Web page identification information in the service providing condition DB 203. Then, the approval or denial judgment unit 205 examines whether the private information described in the user certificate satisfies the service providing conditions (for example, whether qualifications specified by the private information satisfy conditions required for accounting (for example, membership of a credit card)). The approval or denial judgment unit 205 sends the authentication unit 204 the judgment result indicating permission or rejection of browsing the Web page depending on whether the service providing conditions are or are not satisfied (S2017).

[0119] When the judgment result received from the approval or denial judgment unit 205 indicates rejection of browsing the Web page or when the verification of the

signature fails in S2016, then, the authentication unit generates approval or denial information indicating that browsing of the Web page is not permitted, and sends the approval or denial information to the service providing apparatus 30' through the dedicated network IF unit 201. On the other hand, when the judgment result indicates permission to browse the Web page, then, the approval or denial judgment unit 205 generates approval or denial information to that effect, and sends the approval or denial information to the service providing apparatus 30' through the dedicated network IF unit 201 (S2018).

[0120] In the service providing apparatus 30', receiving the approval or denial information from the management apparatus 20' through the dedicated network IF unit 303, the approval or denial information acquisition unit 306 sends the approval or denial information to the repeater unit 304.

[0121] When the approval or denial information received from the approval or denial information acquisition unit 306 indicates permission to browse the Web page, then, the repeater unit 304 sends the accounting unit 308 the Web page identification information specified by the URL included in the browsing request received in S2010, and the certificate identification information received in S2014 by the certificate identification information acquisition unit 305 from the information terminal 40'. Receiving them, the accounting unit 308 adds 1 to the frequency of using the Web page that is associated with the Web page identification information and the certificate identification information received from the repeater unit 304 in the accounting DB 309. Or, the accounting unit 308 registers anew the certificate identification information of the user and the use frequency "1", in association with the above-mentioned Web page identification information, in the accounting DB 309 (S2019).

[0122] Further, when the approval or denial information received from the approval or denial information acquisition unit 306 indicates permission of browsing the Web page, the repeater unit 304 sends the browsing request received in S2010 to the Web server 10' through the Internet IF unit 302. Receiving this, the Web server 10' sends the Web page corresponding to the URL included in the above-mentioned browsing request, to the information terminal 40' through the service providing unit 30', so that the Web page is displayed on the information terminal 40'. On the other hand, when the approval or denial information indicates rejection of browsing the Web page, the repeater unit 304 sends a Web page corresponding to a predetermined URL (for example, a Web page including a message that browsing of the desired Web page is rejected) to the information terminal 40' through the radio IF unit 301, so that the sent Web page is displayed on the information terminal 40' (S2020).

[0123] Hereinabove, the second embodiment of the present invention has been described.

[0124] Similarly to the above-described first embodiment, also the present embodiment can reduce possibility of outflow of private information itself, which is described in a user certificate. Further, it is possible to confirm that the user of the information terminal 40' is a legitimate user specified by the user certificate corresponding to the certificate identification information.

[0125] Further, in the present embodiment, an authentication mark added to a Web page can be used for confirming a relation between the Web page in question and a Web page certified by the authentication mark. Accordingly, from the viewpoint of the user of the information terminal 40', security of using a Web page is improved. In addition, even when, in Fig. 15, the signature verification in S2005 is successful but the coincidence verification in S2006 fails, or, in other words, even when the authentication mark itself is a legitimate one issued by the authentication mark issuer, but there is a good possibility that the authentication mark is used illegally by a third party who does not have a legitimate right of using, advantageously it is possible to move from the authentication mark to the Web page certified by the authentication mark.

[0126] Similarly to the above-described first embodiment, also in the present embodiment, the service providing apparatus 30' may be provided with an authentication unit for verification of a signature to certificate identification information, so that verification of a signature added to the certificate identification information is performed in the service providing apparatus 30' instead of the authentication unit 204 of the management apparatus 20'. In that case, the service providing apparatus 30' may acquire the verification key together with the certificate identification information and the signature to the certificate identification information, from the information terminal 40'.

[0127] Further, in the above-described embodiment, the service providing apparatus 30' may be provided with an approval or denial judgment unit so that the judgment on approval or denial of browsing a Web page is made in the service providing apparatus 30' instead of the approval or denial judgment unit 205 of the management apparatus 20'. In that case, the service providing condition DB 203 of the management apparatus 20' registers private information items required for judgment on approval or denial of browsing a Web page, in association with the Web page identification information concerned. The service providing apparatus 30' is made to send an information transmission request including certificate identification information and Web page identification information, to the management apparatus 20'. Then, with respect to the private information items registered in the service providing condition DB 203 in association with the Web page identification information included in the above-mentioned information transmission request, the management apparatus 20' extracts those private information items from the user certificate registered in the user certificate DB 202 in association

with the certificate identification information included in the above-mentioned information transmission request, and sends the extracted private information items to the service providing apparatus 30'. In this case also, possibility of outflow of private information can be reduced in comparison with the conventional case, since the private information sent to the service providing apparatus 30' is limited to the private information items whose transmission is permitted by the management apparatus 20' (i.e., information items actually required for judgment on Web page browsing).

[0128] Further, in the above-described embodiment, the certificate identification information acquisition unit 105 of the service providing apparatus 30' may have the following function. Namely, prior to acquisition of certificate identification information from an information terminal 40', the certificate identification information acquisition unit 105 displays a message asking whether transmission of the certificate identification information is agreed, or, in other words, whether acting as an agency in accounting of charges for using Web pages is agreed, on the display unit 404 of the information terminal 40'. And, only when the user of the information terminal 40' agrees, the certificate identification information is acquired from the information terminal 40'.

[0129] Further, in the above-described embodiment, the certificate identification information request (S2012) and the processing related to that request may be omitted. In that case, the service providing apparatus 30' may sends a code and the like for identifying the information terminal 40' to the management apparatus 20', so that the management apparatus 20' judges approval for Web browsing, based on the code. Or, the service providing apparatus 30' may perform accounting (S2019) without making a request to the management apparatus 20' for verification.

[0130] Next, a third embodiment of the present invention will be described.

[0131] As the third embodiment of the present invention, will be taken an example in which the authentication system of the present invention is applied to a settlement system in which an information terminal is used in a shop or the like.

[0132] Fig. 21 is a schematic diagram showing an authentication system to which the third embodiment of the present invention is applied. In this figure and Fig. 1 showing the first embodiment, same reference numerals refer to elements having same functions.

[0133] In Fig. 21, a seller terminal 80 is an information terminal installed and used, for example, at a cashier of a shop. The seller terminal 80 has a function of communicating with a service providing apparatus (a settlement apparatus) 70 through the public network 90. The service providing apparatus 70 performs settlement between a consumer as a user of an information terminal 40" and a seller as a user of the seller terminal 80. Here, the service providing apparatus 70 manages account information of a consumer, in association with his certificate identification information, and manages account information of a seller, in association with seller identification information. Further, a management apparatus 20" manages a user certificate, giving it certificate identification information, and manages conditions (possession of membership, and the like, and hereinafter referred to as settlement service providing conditions) for receiving the settlement service provided by the service providing apparatus 70, in association with seller identification information. In Fig. 21, the management apparatus 20" is connected to the service providing apparatus 70 through a dedicated network 60. However, the management apparatus 20" and the service providing apparatus 70 may be connected through a public network 90, when a communication technique (such as cipher communication or the like) that can ensure security is employed.

[0134] In the above-described configuration, when a consumer purchases a commodity in a shop, a seller sends a seller's side settlement request to the service providing apparatus 70, using his seller terminal 80. The seller's side settlement request includes his seller identification information, transaction amount information indicating an amount of transaction (an amount of a consumer's purchase) with a consumer, and a management number (for example, a serial number) that the seller determined uniquely for managing settlement between the consumer and the seller. On the other hand, the consumer sends a consumer's side settlement request to the service providing apparatus 70, using his information terminal 40". The consumer's side settlement request includes his certificate identification information and the above-mentioned management number notified from the seller. When the seller's side settlement request and the consumer's side settlement request having the same management number make a pair, then, the service providing apparatus 70 first sends the management apparatus 20" a verification request, which includes the certificate identification information included in the consumer's side settlement request and the seller identification information included in the seller's side settlement request.

[0135] Receiving the verification request, the management apparatus 20" specifies the user certificate that it manages in association with the certificate identification information included in the verification request, and specifies the settlement service providing conditions that it manages in association with the seller identification information included in the verification request. Then, the management apparatus 20" judges whether the private information described in the specified user certificate satisfies the specified settlement service providing conditions, to determine approval or denial of providing the settlement service, and sends approval or denial information indicating the content of the determination to the service providing apparatus 70.

[0136] When the service providing apparatus 70 receives the approval or denial information from the man-

agement apparatus 20", and the content of the approval or denial information indicates permission to provide the settlement service, then, the service providing apparatus 70 draws the amount of money indicated by the transaction amount information included in the above-mentioned seller's side settlement request from the consumer's account specified by the account identification information managed in association with the certificate identification information included in the above-mentioned consumer's side settlement request, and transfers the drawn amount of money to the seller's account specified by the account identification information managed in association with the seller identification information included in the above-mentioned seller's side settlement request. Then, the processing result is reported to the information terminal 40" and the seller terminal 80. On the other hand, when the content of the approval or denial information indicates rejection of providing the settlement service, then, the service providing apparatus 70 sends a message to that effect to the information terminal 40" and the seller terminal 80.

[0137] Thus, in the present embodiment, a consumer can purchase a commodity at a shop without carrying about money, by using an information terminal 40". Further, in the present embodiment, an information terminal 40" or a seller terminal 80 sends the service providing apparatus 70 certificate identification information as identification information of a user certificate or seller identification information as identification information of a seller. Further, the management apparatus 20" sends the service providing apparatus 70 approval or denial information that indicates approval or denial of providing the settlement service. Namely, a user certificate and private information itself of a seller are not transmitted on the public network 90 and the dedicated network 60. Accordingly, possibility of outflow of a user certificate or private information to a third party can be reduced.

[0138] Next, the service providing apparatus 70' as a component of the system shown in Fig. 21 will be described. In the present embodiment, the management apparatus 20" is similar to the management apparatus 20 of the first embodiment shown in Fig. 3, except that the service providing condition DB 203 registers settlement service providing conditions in association with seller identification information. Further, similarly to the first embodiment shown in Fig. 1,a portable terminal such as a portable telephone or a PDA can be used as the information terminal 40". Further, as the seller terminal 80, can be used an information terminal that has a function of communicating with the service providing apparatus 70 through the public network 90. Further, a radio base station 30" is an ordinary radio base station having a function of connecting the information terminal 40" to the public network 90. Thus, description of the management apparatus 20", the information terminal 40", the seller terminal 80 and the radio base station 30" will be omitted.

[0139] Fig. 22 is a schematic diagram showing the service providing apparatus 70.

[0140] In Fig. 22, a public network IF unit 701 is an interface for communicating with an information terminal 40" and a seller terminal 80 through the public network 90.

[0141] A dedicated network IF unit 702 is an interface for communicating with the management apparatus 20" through the dedicated network 60.

[0142] A consumer account management DB 703 registers account information of a consumer, in association with the certificate identification information of that consumer.

[0143] A seller account management DB 704 registers account information of a seller, in association with seller identification information of that seller.

[0144] A settlement management DB 705 is a database for management of settlement between a consumer and a seller, and, as shown in Fig. 23, registers a record that has a field 7051 for registering a management number, a field 7052 for registering a seller's side settlement request, a field 7053 for registering a consumer's side settlement request, and a field 7054 for registering a settlement state (settled, unsettled, or failure).

[0145] When a settlement processing unit 706 receives a seller's side settlement request from the seller terminal 80 through the public network IF unit 701, then, the settlement processing unit 706 examines whether the settlement management DB 705 has a record in the field 7051 of which the management number included in the seller's side settlement request is registered. When such a record exists (in this case, the consumer's side settlement request and the "unsettled" state are registered into the fields 7053 and 7054, respectively), the settlement processing unit 706 registers the above-mentioned seller's side settlement request into the filed 7052 of this record. And, the below-mentioned settlement is performed. When such a record does not exist, then, the settlement processing unit 706 adds a new record, and registers the above-mentioned management number, the above-mentioned seller's side settlement request and the "unsettled" state into the fields 7051, 7052 and 7054 of this record, respectively.

[0146] When the settlement processing unit 706 receives the consumer's side settlement request from the seller terminal 80 through the public network IF unit 701, the settlement processing unit 706 examines whether the settlement DB 705 has a record in the field 7051 of which the management number included in the consumer's settlement request is registered. When there exists such a record (in this case, the seller's side settlement request and the "unsettled" state are registered into the fields 7052 and 7054, respectively), then, the settlement processing unit 706 registers the above-mentioned consumer's side settlement request into the field 7053 of this record, and performs the below-mentioned settlement processing. When there does not exist such a record, the settlement processing unit 706 adds a new

record and registers the above-mentioned management number, the above-mentioned consumer's side settlement request, and the "unsettled" state into the fields 7051, 7053 and 7054 of the record, respectively.

[0147] Further, the settlement processing unit 706 performs the following settlement processing on the record in the fields 7051, 7052 and 7054 of which the management number, the seller's side settlement request and the consumer's side settlement request, are registered respectively and in the filed 7055 of which the "unsettled" state is registered in the settlement DB 705.

[0148] Namely, the settlement processing unit 706 sends the approval or denial information acquisition unit 707 the seller identification information included in the seller's side settlement request registered in the field 7052 of the record and the certificate identification information added with the signature included in the consumer's side settlement request, to receive approval or denial information from the approval or denial information acquisition unit 707. When the approval or denial information indicates permission to provided the settlement service, then the settlement processing unit 706 draws the amount of money indicated by the transaction amount information included in the above-mentioned seller's side settlement request from the account specified by the account identification information registered in the consumer account management DB 703 in association with the certificate identification information included in the above-mentioned consumer's side settlement request, and transfers the drawn amount to the seller's account specified by the account identification information registered in the seller account management DB 704 in association with the seller identification information included in the above-mentioned seller's side settlement request. Then, the processing result is reported to the information terminal 40" and the seller terminal 80 through the public network IF unit 701, and the settlement processing unit 706 updates the settlement state registered in the field 7054 of the record (in this case, into "settled" or "failure"). On the other hand, when the approval or denial information indicate rejection of providing the settlement service, then, the settlement processing unit 706 sends a message to that effect to the information terminal 40" and the seller terminal 80 through the public network IF unit 701, and updates the settlement state registered in the field 7054 of the record (in this case, into "failure").

[0149] When the approval or denial information acquisition unit 707 receives the seller identification information and the certificate identification information added with the signature from the settlement processing unit 706, then, the approval or denial information acquisition unit 707 generates a settlement request including them and sends the settlement request to the management apparatus 20" through the dedicated network IF unit 702. And, the approval or denial information acquisition unit 707 receives approval or denial information from the management apparatus 20" as a response to the verification request, and sends the received approval or denial information to the settlement processing unit 706.

[0150] Similarly to the service providing apparatus 10 of the first embodiment, also the service providing apparatus 70 having the above-described configuration may be implemented, for example, by a computer system having a configuration such as shown in Fig. 7 or by a network system comprising a plurality of such computer systems connected with one another through a network.

[0151] Next, operation of the authentication system of the above-described configuration will be described.

[0152] Fig. 24 is a diagram for explaining an operating procedure of the authentication system shown in Fig. 21.

[0153] When a consumer demands purchase of a commodity from a seller, the seller notifies the consumer of the amount of money to pay for the commodity and a unique management number generated by using a seller terminal 80 or the like. At the same time, the seller inputs transaction amount information, which indicates the amount of money to pay for the commodity, into the seller terminal 80 (S2301). Receiving the input, the seller terminal 80 generates a seller's side settlement request including the above-mentioned transaction amount information, the above-mentioned management number, and the seller identification information (which is registered in advance) of the seller, and sends the generated seller's side settlement request to the service providing apparatus 70 (S2302).

[0154] In the service providing apparatus 70, when the settlement processing unit 706 receives the seller's side settlement request from the seller terminal 80 through the public network IF unit 701, the settlement processing unit 706 examines whether the settlement DB 705 registers a record whose field 7051 registers the management number included in the seller's side settlement request. When it is confirmed that such a record is not registered, the settlement processing unit 706 adds a new record to the settlement DB 705, and registers the above-mentioned management number, the above-mentioned seller's side settlement request, and the settlement state of "unsettled" into the fields 7051, 7052 and 7054 of the new record (S2303).

[0155] On the other hand, the consumer inputs the management number, which has been notified by the seller, into his information terminal 40" (S2304). Receiving the input, the information terminal 40" generates a signature to the consumer's certificate identification information (which has been registered in advance) using a signature key (which also has been registered in advance) (S2305). Then, the information terminal 40" generates a consumer's side settlement request including the above-mentioned management number and the certificate identification information added with the above-mentioned signature, and sends the generated request to the service providing apparatus 70 (S2306).

[0156] In the service providing apparatus 70, when

the settlement processing unit 706 receives the consumer's side settlement request from the information terminal 40" through the public network IF unit 701, then, the settlement processing unit 706 examines whether the settlement DB 705 has a record in the field 7051 of which the management number included in the consumer's side settlement request is registered. When it is confirmed that such a record is registered, then, the settlement processing unit 706 registers the above-mentioned consumer's side settlement request into the field 7053 of the record (S2307). Now, the record in question (hereinafter, referred to as the object record) registers all the information required for settlement.

[0157] Then, the settlement processing unit 706 sends the approval or denial information acquisition unit 707 the seller identification information (which is included in the seller's side settlement request registered in the field 7052 of the object record) and the certificate identification information added with the signature (which is included in the consumer's side settlement request registered in the field 7053). Receiving them, the approval or denial information acquisition unit 707 generates a verification request including the above-mentioned seller identification information and the above-mentioned certificate identification information added with the signature, and sends the generated verification request to the management apparatus 20" through the dedicated network IF unit 702 (S2308).

[0158] In the management apparatus 20", when the authentication unit 204 receives the verification request from the service providing apparatus 70 through the dedicated network IF unit 201, then, the authentication unit 204 reads the verification key registered in the user certificate DB 202 in association with the certificate identification information included in the verification request. Then, using the verification key, the authentication unit 204 verifies the signature to the certificate identification information, which is included in the verification request (S2309). When the verification of the signature is successful, the authentication unit 204 sends the certificate identification information and the seller identification information included in the verification request to the approval or denial judgment unit 205.

[0159] Receiving them, the approval or denial judgment unit 205 reads the user certificate registered in association with the certificate identification information in the user certificate DB 202, and the settlement service providing conditions registered in association with the seller identification information in the service providing condition DB 203. Then, the approval or denial judgment unit 205 examines whether the private information described in the user certificate satisfies the settlement service providing conditions (for example, whether the consumer is a member who can receive the settlement service). The approval or denial judgment unit 205 sends the authentication unit 204 the judgment result to the effect that enjoyment of the settlement service is permitted or rejected, depending on whether the settlement service providing conditions are satisfied, or are not satisfied (S2310).

[0160] When the judgment result received from the approval or denial judgment unit 205 indicates rejection of providing the settlement service, or when the signature verification in S2309 fails, then, the authentication unit 204 generates approval or denial information indicating rejection of providing the settlement service and sends the generated approval or denial information to the service providing apparatus 70 through the dedicated network IF unit 201. On the other hand, when the judgment result received from the approval or denial judgment unit 205 indicates permission to provide the settlement service, then, the authentication unit 204 generates approval or denial information to that effect, and sends the approval or denial information to the service providing apparatus 70 through the dedicated network IF unit 201 (S2311).

[0161] In the service providing apparatus 70, when the approval or denial information acquisition unit 707 receives the approval or denial information from the management apparatus 20" through the dedicated network IF unit 702, then, the approval or denial information acquisition unit 707 sends it to the settlement processing unit 706. When the approval or denial information received from the approval or denial information acquisition unit 707 indicates permission to provide the settlement service, the settlement processing unit 706 draws the amount of money indicated by the transaction amount information included in the seller's side settlement request registered in the field 7052 of the object record from the account specified by the account identification information registered in the consumer account management DB 703 in association with the certificate identification information included in the consumer's side settlement request registered in the field 7053 of the object record. Then, the settlement processing unit 706 transfers the drawn amount to the seller's account specified by the account identification information registered in the seller account management DB 704 in association with the seller identification information included in the above-mentioned seller's side settlement request, and updates the settlement state registered in the field 7054 of the object record. Then, the settlement processing unit 706 reports the processing result to the information terminal 40" and the seller terminal 80 through the public network IF unit 701 (S2312).

[0162] On the other hand, when the approval or denial information received from the approval or denial information acquisition unit 707 indicates rejection of providing the settlement service, then, the settlement processing unit 706 sends a message to that effect to the information terminal 40" and the seller terminal 80 through the public network IF unit 701, and, at the same time, updates the settlement state registered in the field 7054 of the object record (S2313).

[0163] When it is confirmed that the settlement has normally finished, from the message received from the

service providing apparatus 70 through the seller terminal 80, the seller delivers the commodity to the consumer.

[0164] Hereinabove, the third embodiment of the present invention has been described.

[0165] According to the present embodiment, a consumer can use an information terminal 40" to purchase a commodity at a shop, without carrying about money. Further, in the present embodiment, the information terminal 40" or the seller terminal 80 sends certificate identification information of a user certificate and seller identification information of a seller, to the service providing apparatus 70. Further, the management apparatus 20" sends the service providing apparatus 70 approval or denial information, which indicates approval or denial of providing the settlement service. Thus, a user certificate and private information itself are not transmitted on the public network 90 and the dedicated network 60. Accordingly, possibility of outflow of a user certificate or private information to a third party can be reduced.

[0166] In the above embodiment, the service providing apparatus 70 may be provided with an authentication unit for verification of a signature, so that verification of a signature added to certificate identification information is performed in the service providing apparatus 70 instead of the authentication unit 204 of the management apparatus 20". In that case, the service providing apparatus 70 may acquire a verification key together with a signature to the certificate identification information, from the information terminal 40".

[0167] Further, in the above embodiment, the service providing apparatus 70 may be provided with an approval or denial judgment unit, so that the judgment of approval or denial of providing the settlement service is performed in the service providing apparatus 70 instead of the approval or denial judgment unit 205 of the management apparatus 20". In that case, the service providing condition DB 203 of the management apparatus 20" registers private information items required for judgment on approval or denial of providing the settlement service, in association with seller identification information concerned. The service providing apparatus 70 sends the management apparatus 20" an information transmission request including certificate identification information and seller identification information. Then, with respect to the private information items registered in the service providing condition DB 203 in association with the seller identification information included in the above-mentioned information transmission request, the management apparatus 20" extracts those private information items from the user certificate registered in the user certificate DB 202 in association with the certificate identification information included in the above-mentioned information transmission request. The management apparatus 20" sends the extracted private information items to the service providing apparatus 70. In this arrangement also, possibility of outflow of private information can be reduced in comparison with the conventional case, since the private information sent to the service providing apparatus 70 is limited to the private information items whose transmission is permitted by the management apparatus 20" (i.e., information items actually required for judgment on providing the settlement service).

[0168] Further, in the above-described embodiment, the transaction amount information is sent to the service providing apparatus 70, being included only in the seller's side settlement request sent from the seller terminal 80. However, the transaction amount may be sent to the service providing apparatus 70, being included also in the consumer's side settlement request sent from the information terminal 40", so that the service providing apparatus 70 examines whether the transaction amount information included in the seller's side settlement request coincides with the transaction amount information included in the consumer's side settlement request.

[0169] Further, in the above-described embodiment, the service providing apparatus 70 sends the result of the settlement service, to both the seller terminal 80 and information terminal 40". However, the result of the settlement service may be sent to the seller terminal 80 only. Then, the seller may show the display screen or the like of the seller terminal 80 to the consumer as the user of the terminal 40", in order to inform the consumer of the result of the settlement service.

[0170] Further, the above-described embodiment may be modified such that settlement is performed when the information terminal 40" sends a seller's side settlement request to the service providing apparatus 70.

[0171] Fig. 25 is a diagram for explaining a variant of the operating procedure of the authentication system shown in Fig. 21.

[0172] When a consumer demands purchase of a commodity from a seller, the seller notifies the consumer of the seller identification information, the amount of money to pay for the commodity and a unique management number generated by using a seller terminal 80 or the like. The consumer inputs the management number, the amount of money to pay for the commodity and the seller identification information notified from the seller, into his information terminal 40" (S2401). Receiving the input, the information terminal 40" generates a signature to the certificate identification information registered in advance, using the signature key registered in advance (S2402). Then, the information terminal 40" generates a consumer's side settlement request including the above-mentioned management number and the certificate identification information added with the above-mentioned signature, generates a seller's side settlement request including the above-mentioned management number, above-mentioned transaction amount information and the above-mentioned seller identification information, and sends those requests to the service providing apparatus 70 (S2403).

[0173] In the service providing apparatus 70, the set-

tlement processing unit 706 receives the consumer's side settlement request and the seller's side settlement request from the information terminal 40" through the public network IF unit 701, then, the settlement processing unit 706 adds a new record to the settlement DB 705, and registers the management number, the above-mentioned seller's side settlement request and the above-mentioned consumer's side settlement request included in those settlement requests into the fields 7051 - 7053 of the new record. Further, the settlement processing unit 706 registers the settlement state "unsettled" into the field 7054 of the record (S2404). Thus, all the information required for settlement has been registered into the record (hereinafter, referred to as the object record).

[0174] Then, the settlement processing unit 706 sends the approval or denial information acquisition unit 707 the seller identification information (which is included in the seller's side settlement request registered in the field 7052 of the object record) and the certificate identification information added with the signature (which is included in the consumer's side settlement request registered in the field 7053). Receiving them, the approval or denial information acquisition unit 707 generates a verification request including the above-mentioned seller identification information and the above-mentioned certificate identification information added with the signature, and sends the generated verification request to the management apparatus 20" through the dedicated network IF unit 702 (S2405).

[0175] Then, the apparatus 20" performs processing similar to the S2309 and S2310 of Fig. 24, and approval or denial information is sent to the service providing apparatus 70 (S2406 - S2408).

[0176] In the service providing apparatus 70, when the approval or denial information acquisition unit 707 receives the approval or denial information from the management apparatus 20" through the dedicated network IF unit 702, then, the approval or denial information acquisition unit 707 sends the approval or denial information to the settlement processing unit 706. When the approval or denial information received from the approval or denial information acquisition unit 707 indicates permission to provide the settlement service, then, the settlement processing unit 706 draws the amount of money indicated by the transaction amount information included in the seller's side settlement request registered in the field 7052 of the object record, from the account specified by the account identification information registered in the consumer account management DB 703 in association with the certificate identification information included in the consumer's side settlement request registered in the field 7053 of the object record. Then, the settlement processing unit 706 transfers the drawn amount into the seller's account specified by the account identification information registered in the seller account management DB 704 in association with the seller identification information included in the above-mentioned seller's side settlement request, and updates the settlement state registered in the field 7054 of the object record (S2409).

[0177] Then, the settlement processing unit 706 generates payment confirmation information according to predetermined rules, using the information of the seller's side settlement request registered in the field 7052 of the object record. For example, the settlement processing unit 706 generates the payment confirmation information, by connecting the management number, the seller identification information and the transaction amount information. Then, using a key for evaluated value, which is registered in advance, the settlement processing unit 706 generates an evaluated value (for example, a hash value) to the payment confirmation information (S2410), and sends the evaluated value to the information terminal 40" through the public network IF unit 701 (S2411).

[0178] Receiving the evaluated value from the service providing apparatus 70, the information terminal 40" displays the evaluated value on the display unit (S2412). The consumer presents the displayed content to the seller. Receiving this and using the seller terminal 80, the seller generates payment confirmation information from the management number, the seller identification information and the transaction amount information, according to the same rules as ones employed by the settlement processing unit 706 of the service providing apparatus 70. Then, using the key for evaluated value (the same key as the above-mentioned key for evaluated value, which is registered in the service providing apparatus 70 in association with the seller identification information of the seller), which is registered in advance, the evaluated value to the payment confirmation information is generated, and it is examined whether this evaluated value coincides with the evaluated value received from the service providing apparatus 70 (S2413). After the coincidence is confirmed, the commodity is delivered to the consumer.

[0179] Here, in S2410 and S2411, instead of generating the evaluated value, the settlement processing unit 706 may generate a signature to the payment confirmation information, using a signature key of the user of the service providing apparatus 70, and send the signature and the payment confirmation information to the information terminal 40", to make the information terminal 40" display the signature. Then, in S2413, an optical reader optically reads the signature and the payment confirmation information displayed on the information terminal 40", to take them into the seller terminal 80. Then, the seller terminal verifies the signature, using the verification key (which is registered in advance) of the user of the service providing apparatus 70.

[0180] Hereinabove, various embodiments of the present invention have been described.

[0181] The present invention is not limited to the above-described embodiments, and various variations can be obtained within the scope of the invention.

[0182] For example, although the above-described

embodiment supposes that a portable terminal is used as the information terminal, the present invention is not limited to this. For example, in the cases of the above-described first and second embodiments, a fixed-type information terminal may be employed. Further, in the above-described embodiments, a signature to the certificate identification information and verification of the signature are not indispensable.

[0183] Further, the authentication system of the present invention can be widely applied to various service systems (systems of the type where a service providing apparatus provides service to an information terminal or a user of an information terminal) other than the service providing systems described in the above embodiments.

[0184] As described above, according to the present invention, it is possible to reduce possibility of outflow of private information in authentication of a user of an information terminal.

Claims

1. An authentication system comprising a management apparatus that manages private information and a service providing apparatus that provides service to an information terminal, wherein:

said management apparatus comprises:

a private information database in which private information is registered, associating the private information with personal identification information therein;

a providing condition database in which service providing conditions required for private information are registered when said service providing apparatus provides the service therein;

a determination processing unit that reads the private information associated with personal identification information sent from said service providing apparatus, from said private information database, makes a judgment on whether said private information satisfies the service providing conditions registered in said providing condition database, and determines approval or denial of providing the service depending on a result of the judgment; and

a notification processing unit that notifies said service providing apparatus of approval or denial information indicating the judgment result of said determination processing unit, and

said service providing apparatus comprises:

a personal identification information acquisition processing unit that acquires personal identification information from said information terminal;

an approval or denial information acquisition processing unit that sends the personal identification information acquired by said personal identification information acquisition processing unit to said management apparatus, to acquire approval or denial information from said management apparatus; and

a service providing processing unit that provides the service to said information terminal when the approval or denial information acquired by said approval or denial information acquisition processing unit indicates permission to provide the service.

2. The authentication system according to Claim 1, wherein:

said private information database of said management apparatus, in which the private information together with a public key certificate is registered, associating said private information and said public key certificate with the personal identification information;

said determination processing unit of said management apparatus verifies signature information added to the personal identification information sent from said service providing apparatus, using the public key certificate registered in association with said personal identification information in said private information database; performs said judgment when the verification is successful; determines approval or denial of providing the service depending on the result of the judgment; and, on the other hand, determines rejection of providing the service when the verification fails;

said personal identification information acquisition processing unit of said service providing apparatus acquires the personal identification information added with the signature information, from said information terminal; and

said approval or denial information acquisition processing unit of said service providing apparatus sends said management apparatus the personal identification information added with the signature information, which is acquired by said personal identification information acquisition processing unit, to acquire the approval or denial information from said management apparatus.

3. The authentication system according to Claim 2, wherein:

said information terminal has a function as a Web browser;
said service providing apparatus has a function as a Web server;
said service providing processing unit of said service providing apparatus permits said information terminal to browse a certain Web page, when the approval or denial information acquired by said approval or denial information acquisition processing unit indicates permission to provide the service.

4. The authentication system according to Claim 2, wherein:

said information terminal has a function as a Web browser;
said service providing apparatus has a network connecting function for connecting said information terminal to Web server through a network; and
said service providing processing unit of said service providing apparatus permits said information terminal to browse a certain Web page provided by said Web server, when the approval or denial information acquired by said approval or denial information acquisition processing unit indicates permission to provide the service.

5. The authentication system according to Claim 4, wherein:

said certain Web page is a pay content;
said service providing processing unit of said service providing apparatus performs accounting for use of said certain Web page by said information terminal that is permitted to browse said certain Web page.

6. The authentication system according to Claim 5, wherein:

said Web server, holding said certain Web page, holds a Web page including image information to which said certain Web page is set, in a state that said information terminal can browse said Web page including the image information.

7. The authentication system according to Claim 6, wherein:

said image information is set with a link, such that a select action of said image information of an operator of said information terminal causes the identification information of said certain Web page is sent together with identification information of said Web page including the image information under browsing by said information terminal, from said information terminal to said service providing apparatus;
said service providing apparatus further comprises:

a relation information acquisition processing unit that sends said management apparatus the identification information of said certain Web page and the identification information of said Web page including the image information; acquires information on a relation between said certain Web page and said Web page including the image information; and sends the acquired information to said information terminal; and
said management apparatus further comprises:

a Web page identification information database, in which the identification information of said certain Web page is registered, associating said identification information with the identification information of said Web page including the image information to which said identification information of said certain Web page is set; and
a verification processing unit that verifies the relation between said certain Web page and said Web page including the image information, by examining whether the identification information of said certain Web page and the identification information of said Web page including the image information (both sent from said service providing apparatus) are registered in association with each other in said Web page identification information database; and notifies said service providing apparatus of a result of verification.

8. The authentication system according to Claim 2, wherein:

said service providing apparatus further comprises:

a settlement request acquisition processing unit that receives a settlement request (which includes seller identification information, transaction amount information

and a management identification information) from a seller terminal;

a consumer account management database in which an account is registered, associating the account with personal identification information; and

a seller account management database in which an account is registered, associating the account with seller identification information;

said personal identification information acquisition processing unit of said service providing apparatus acquires the personal identification information together with management identification information from said information terminal; and

when the approval or denial information acquired by said approval or denial information acquisition processing unit indicates permission to provide the service, then,

with respect to a settlement request that is acquired by said settlement request acquisition processing unit and that includes the management identification information acquired together with said personal identification information by said personal identification information acquisition processing unit,

said service providing processing unit of said service providing apparatus draws an amount of money indicated by the transaction amount information included in said settlement request, from an account registered in said consumer account management database in association with the personal identification information acquired by said personal identification information acquisition processing unit; transfers the drawn amount of money to an account registered in said seller account management database in association with the seller identification information included in said settlement request; and notifies said seller terminal of a transfer result.

9. The authentication system according to Claim 2, wherein:

said service providing apparatus further comprises: a consumer account management database in which an account is registered, associating the account with personal identification information; and a seller account management database in which an account is registered, associating the account with seller identification information;

said personal identification information acquisition processing unit of said service providing apparatus acquires a settlement request that includes the personal identification information, seller identification information and transaction amount information, from said information terminal; and

when the approval or denial information acquired by said approval or denial information acquisition processing unit indicates permission to provide the service, then,

said service providing processing unit of said service providing apparatus draws an amount of money indicated by the transaction amount information included in the settlement request acquired by said personal information acquisition processing unit, from an account registered in said consumer account management database in association with the personal identification information included in said settlement request; transfers the drawn amount of money to an account registered in said seller account management database in association with the seller identification included in said settlement information; and notifies said information terminal of a transfer result.

10. A method of authentication, in which authentication of an information terminal to which service can be provided is performed using an authentication system comprising a management apparatus that manages private information and a service providing apparatus that provides the service to the information terminal, wherein said method comprises:

a first step in which said service providing apparatus acquires personal identification information from said information terminal, and sends acquired personal identification information to said management apparatus;

a second step in which said management apparatus judges whether private information that the management apparatus manages in association with the personal identification information received from said service providing apparatus satisfies predetermined service providing conditions, and determines approval or denial of providing the service depending on a result of judgment;

a third step in which said management apparatus sends approval or denial information, which indicates a content of the determination of approval or denial of providing the service, to said service providing apparatus; and

a fourth step in which said service providing apparatus provides the service to said information terminal, only when the approval or denial information sent from said management apparatus indicates permission to provide the service.

11. The method of authentication according to Claim 10, wherein:

said information terminal has a function as a Web browser;
said service providing apparatus has a function as a Web server; and
in said fourth step, a certain Web page is provided to said information terminal, when the approval or denial information sent from said management apparatus indicates permission to provide the service.

12. The method of authentication according to Claim 10, wherein:

said information terminal has a function as a Web browser;
said service providing apparatus has a network connecting function for connecting said information terminal to a Web server through a network; and
in said fourth step, said information terminal is enabled to browse a certain Web page provided by said Web page, when the approval or denial information sent from said management apparatus indicates permission to provide the service.

13. The method of authentication according to Claim 12, wherein:

said certain Web page is a pay content; and
said method further comprises:

a fifth step in which said service providing apparatus performs accounting for use of said certain Web page by said information terminal that is permitted to browse said certain Web page.

14. The method of authentication according to Claim 10, wherein:

said method further comprises:

a fifth step in which said service providing apparatus receives a settlement request (which includes seller identification information, transaction amount information and management identification information) from a seller terminal, prior to said first step;
in said first step, personal identification information is received together with the management identification information from said information terminal;
in said fourth step, when the approval or denial information received from said management apparatus indicates permission to provide the service, then, an amount of money indicated by the transaction amount information included in the settlement request that is received from said seller terminal and that includes the management identification information acquired together with the personal identification information from said information terminal is drawn from an account managed in association with the personal identification information acquired from said information terminal; said amount of money is transferred to an account managed in association with the seller identification information included in said settlement request; and a result of transfer is notified to said seller terminal.

15. The authentication method according to Claim 10, wherein:

in said first step, a settlement request, which includes personal identification information, seller identification information and transaction amount information, is acquired from said information terminal;
in said fourth step, when the approval or denial information acquired from said management apparatus indicates permission to provide the service, then, an amount of money indicated by the transaction amount information included in the settlement request that is acquired from said information terminal is drawn from an account managed in association with the personal identification information included in said settlement request; said amount of money is transferred to an account managed in association with the seller identification information included in said settlement request; and a result of transfer is notified to said information terminal.

FIG.1

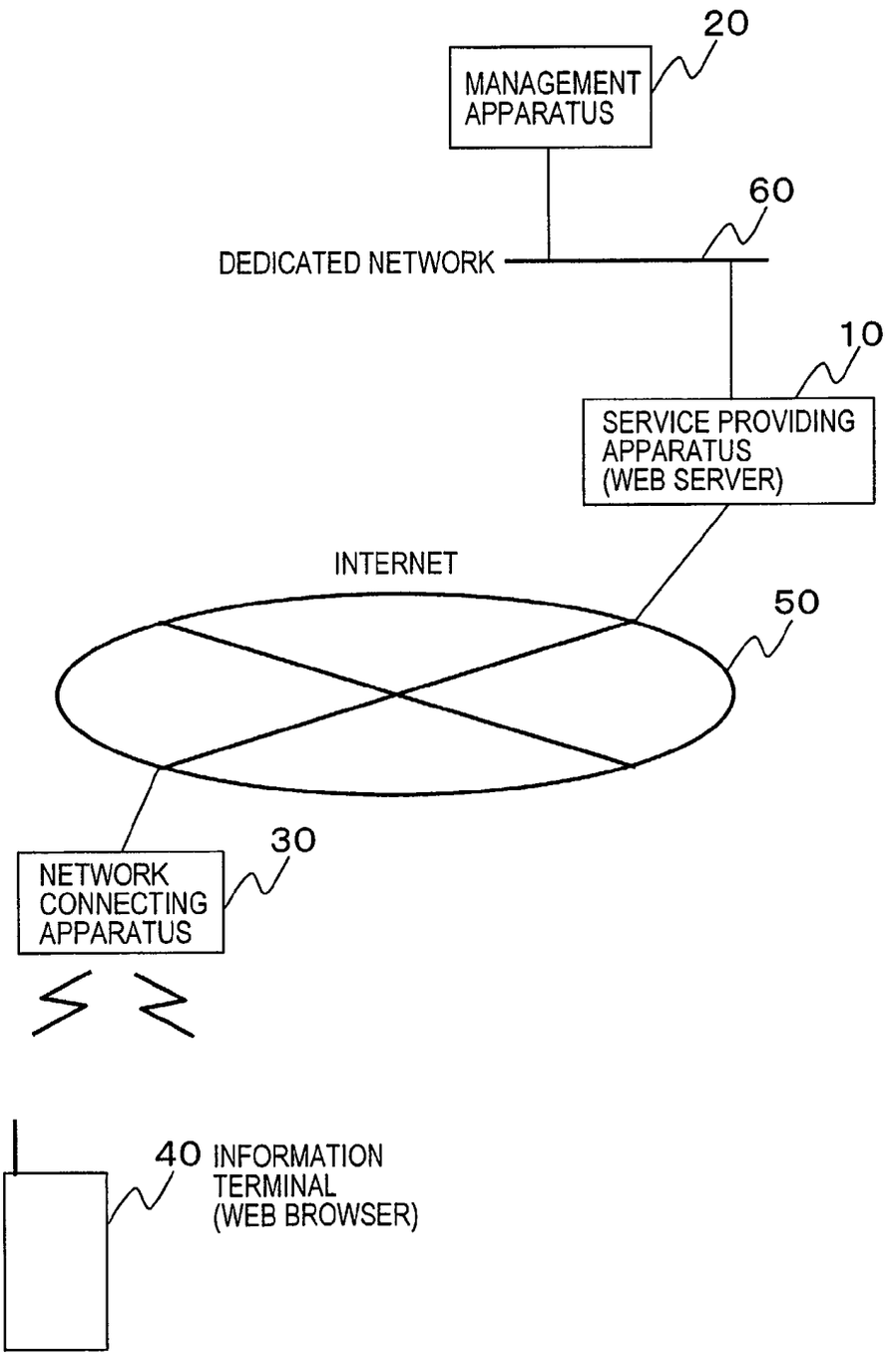

20
MANAGEMENT APPARATUS
60
DEDICATED NETWORK
10
SERVICE PROVIDING APPARATUS (WEB SERVER)
INTERNET
50
30
NETWORK CONNECTING APPARATUS
40
INFORMATION TERMINAL (WEB BROWSER)

FIG.2

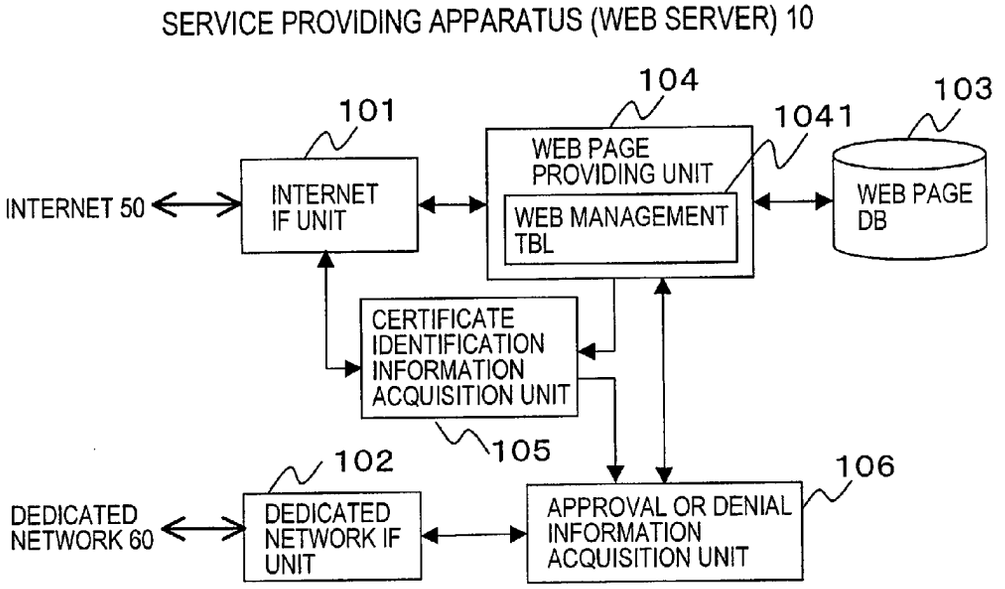

SERVICE PROVIDING APPARATUS (WEB SERVER) 10
101
104
1041
103
INTERNET 50
INTERNET IF UNIT
WEB PAGE PROVIDING UNIT
WEB MANAGEMENT TBL
WEB PAGE DB
CERTIFICATE IDENTIFICATION INFORMATION ACQUISITION UNIT
105
102
106
DEDICATED NETWORK 60
DEDICATED NETWORK IF UNIT
APPROVAL OR DENIAL INFORMATION ACQUISITION UNIT

FIG.3

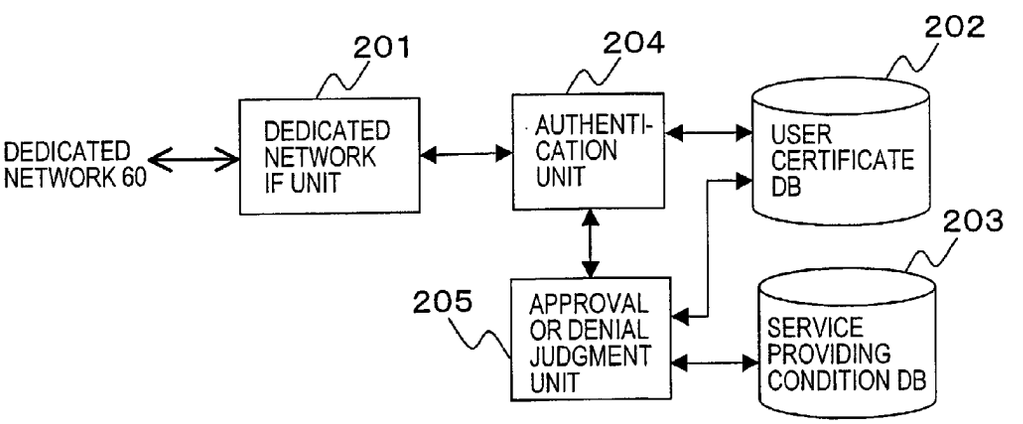
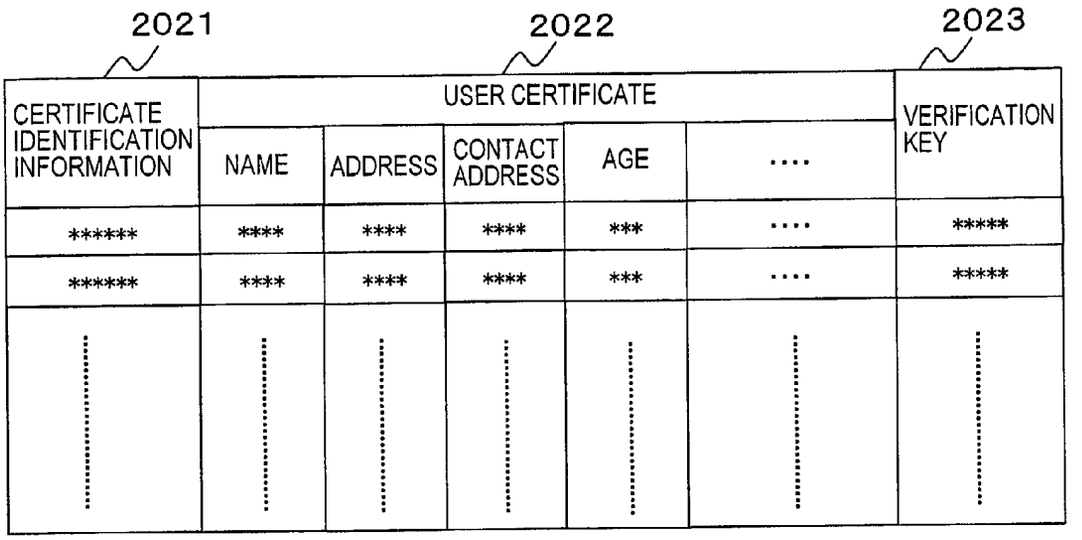

MANAGEMENT APPARATUS 20
201
204
202
DEDICATED NETWORK 60
DEDICATED NETWORK IF UNIT
AUTHENTI-CATION UNIT
USER CERTIFICATE DB
203
205
APPROVAL OR DENIAL JUDGMENT UNIT
SERVICE PROVIDING CONDITION DB

FIG.4

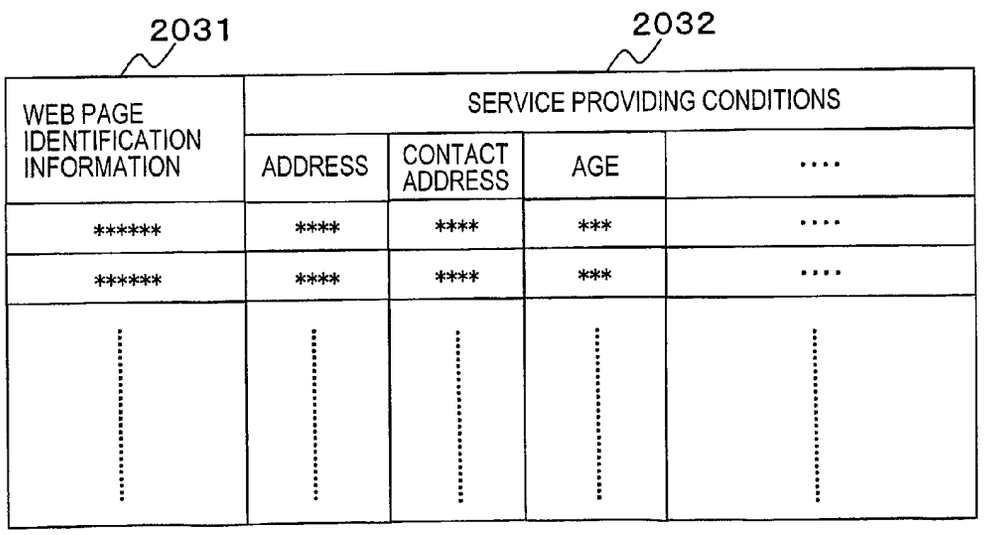
USER CERTIFICATE DB 202



CERTIFICATE IDENTIFICATION INFORMATION	USER CERTIFICATE					VERIFICATION KEY
	NAME	ADDRESS	CONTACT ADDRESS	AGE	....	
******	****	****	****	***	....	*****
******	****	****	****	***	....	*****
⋮	⋮	⋮	⋮	⋮	⋮	⋮

FIG.5

SERVICE PROVIDING CONDITION DB 203



WEB PAGE IDENTIFICATION INFORMATION	SERVICE PROVIDING CONDITIONS			
	ADDRESS	CONTACT ADDRESS	AGE	....
******	****	****	***	....
******	****	****	***	....
⋮	⋮	⋮	⋮	⋮

FIG.6

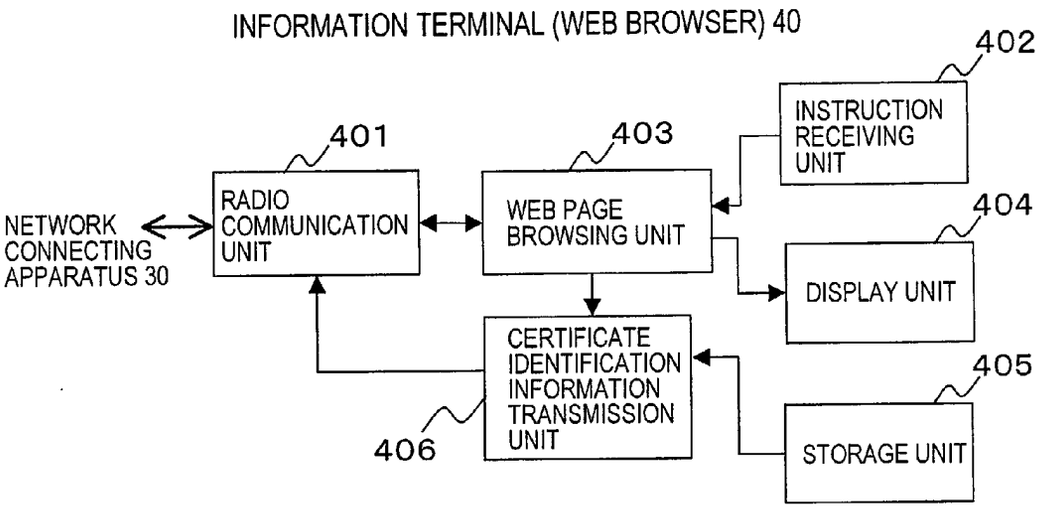

INFORMATION TERMINAL (WEB BROWSER) 40
401
RADIO COMMUNICATION UNIT
NETWORK CONNECTING APPARATUS 30
403
WEB PAGE BROWSING UNIT
402
INSTRUCTION RECEIVING UNIT
404
DISPLAY UNIT
405
STORAGE UNIT
406
CERTIFICATE IDENTIFICATION INFORMATION TRANSMISSION UNIT

FIG.7

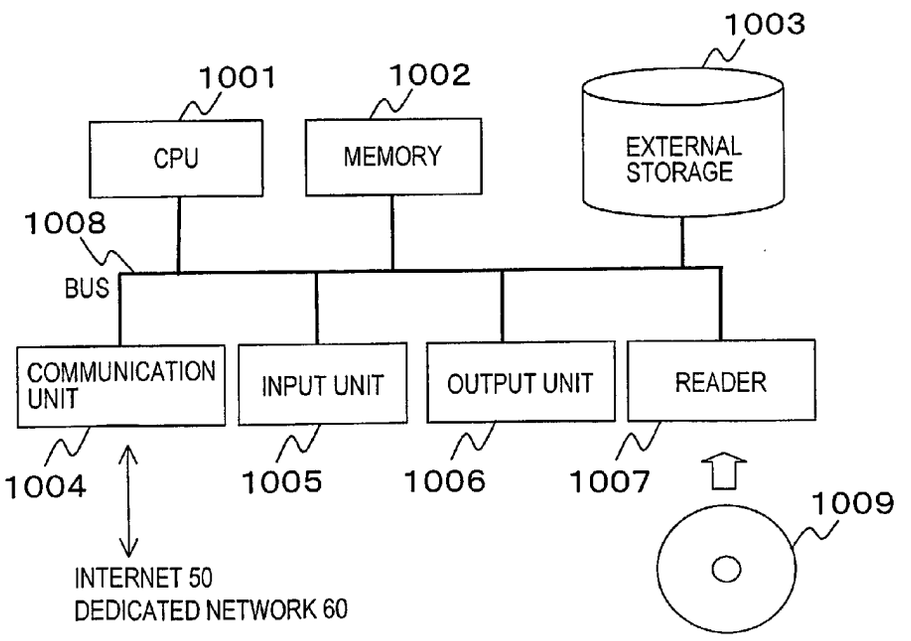

1001
CPU
1002
MEMORY
1003
EXTERNAL STORAGE
1008
BUS
COMMUNICATION UNIT
INPUT UNIT
OUTPUT UNIT
READER
1004
1005
1006
1007
1009
INTERNET 50
DEDICATED NETWORK 60

FIG.8

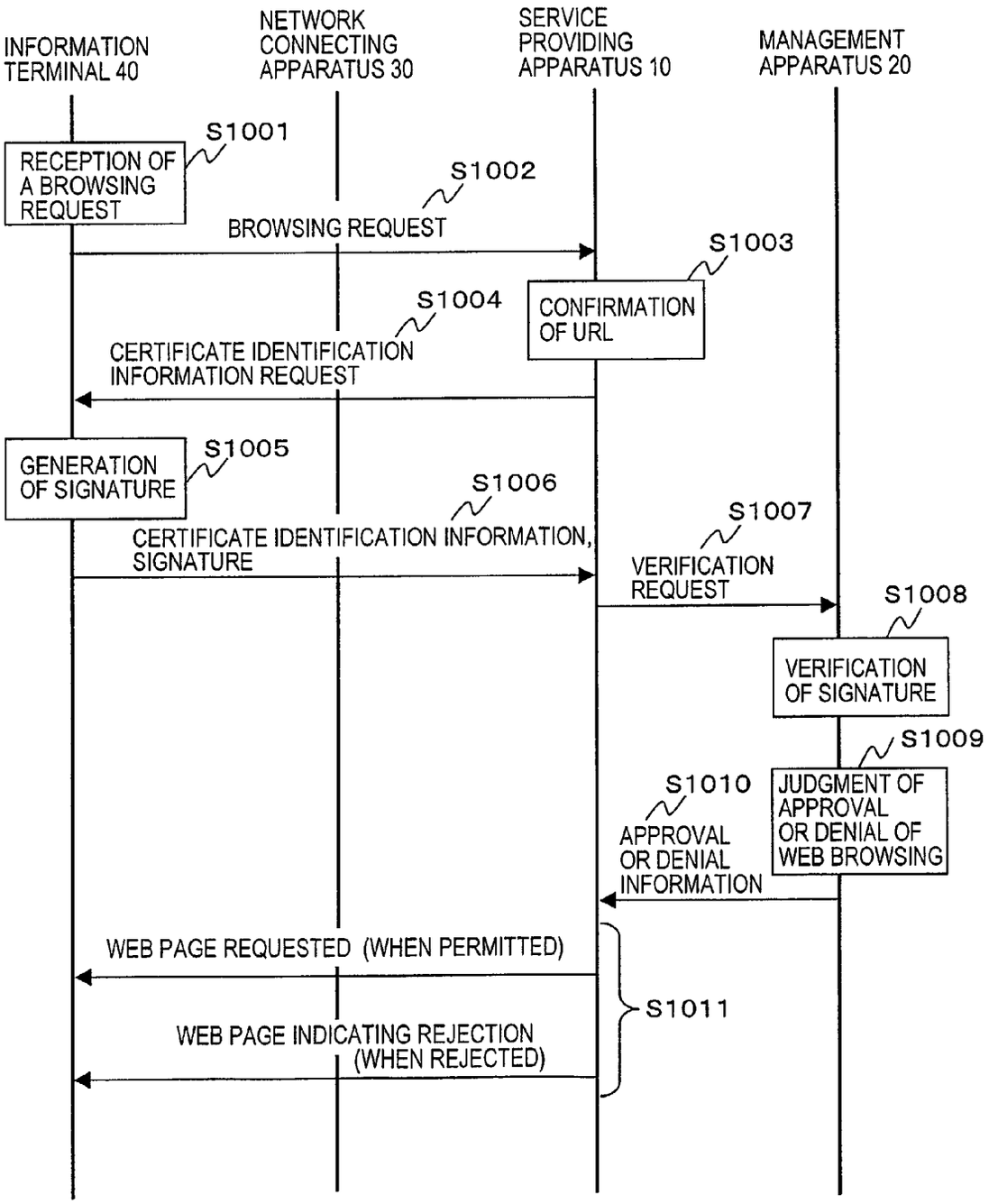

INFORMATION TERMINAL 40
NETWORK CONNECTING APPARATUS 30
SERVICE PROVIDING APPARATUS 10
MANAGEMENT APPARATUS 20
S1001
RECEPTION OF A BROWSING REQUEST
S1002
BROWSING REQUEST
S1003
CONFIRMATION OF URL
S1004
CERTIFICATE IDENTIFICATION INFORMATION REQUEST
S1005
GENERATION OF SIGNATURE
S1006
CERTIFICATE IDENTIFICATION INFORMATION, SIGNATURE
S1007
VERIFICATION REQUEST
S1008
VERIFICATION OF SIGNATURE
S1009
JUDGMENT OF APPROVAL OR DENIAL OF WEB BROWSING
S1010
APPROVAL OR DENIAL INFORMATION
WEB PAGE REQUESTED (WHEN PERMITTED)
WEB PAGE INDICATING REJECTION (WHEN REJECTED)
S1011

FIG.9

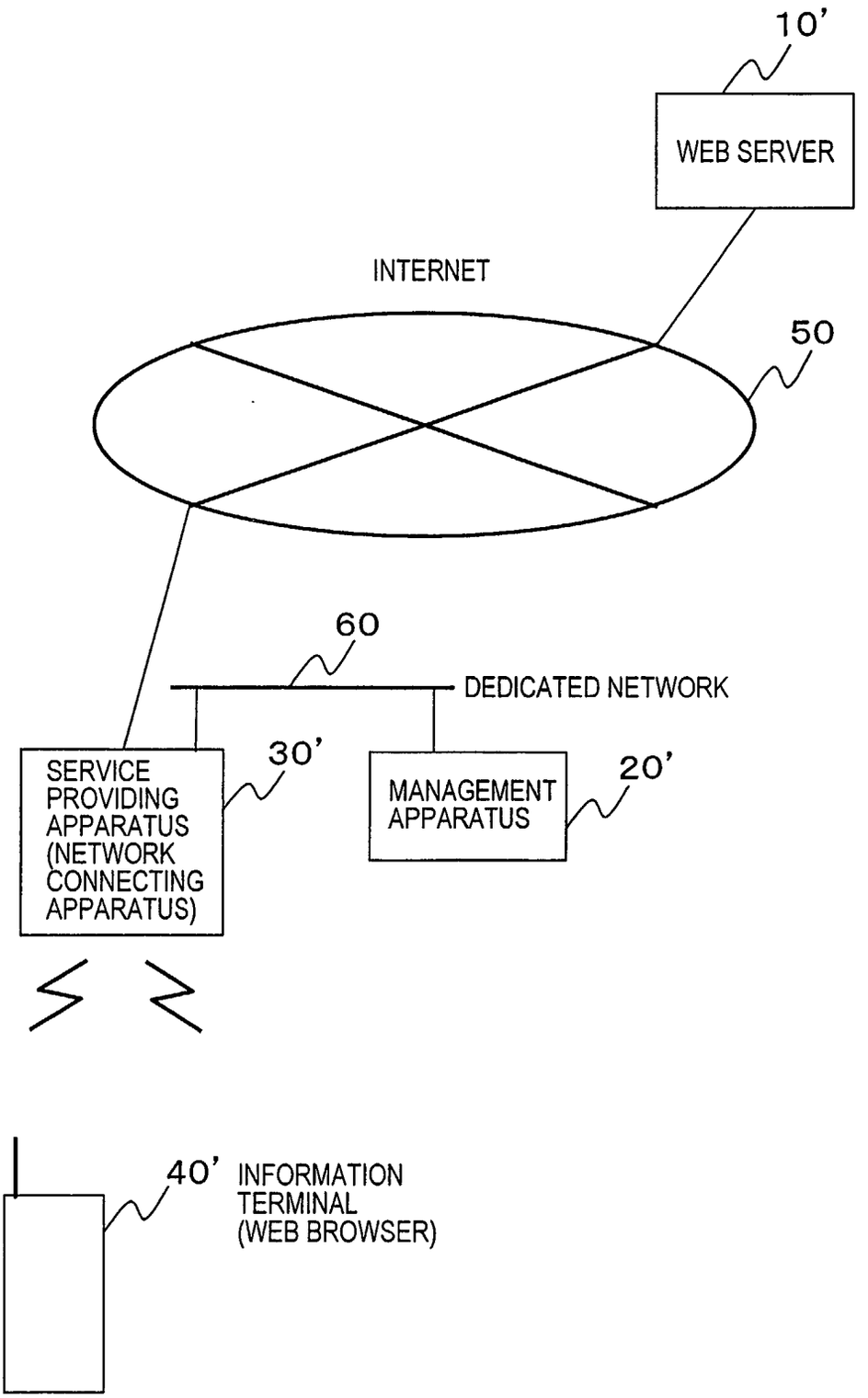

10'
WEB SERVER
INTERNET
50
60
DEDICATED NETWORK
30'
SERVICE PROVIDING APPARATUS (NETWORK CONNECTING APPARATUS)
20'
MANAGEMENT APPARATUS
40'
INFORMATION TERMINAL (WEB BROWSER)

FIG.10

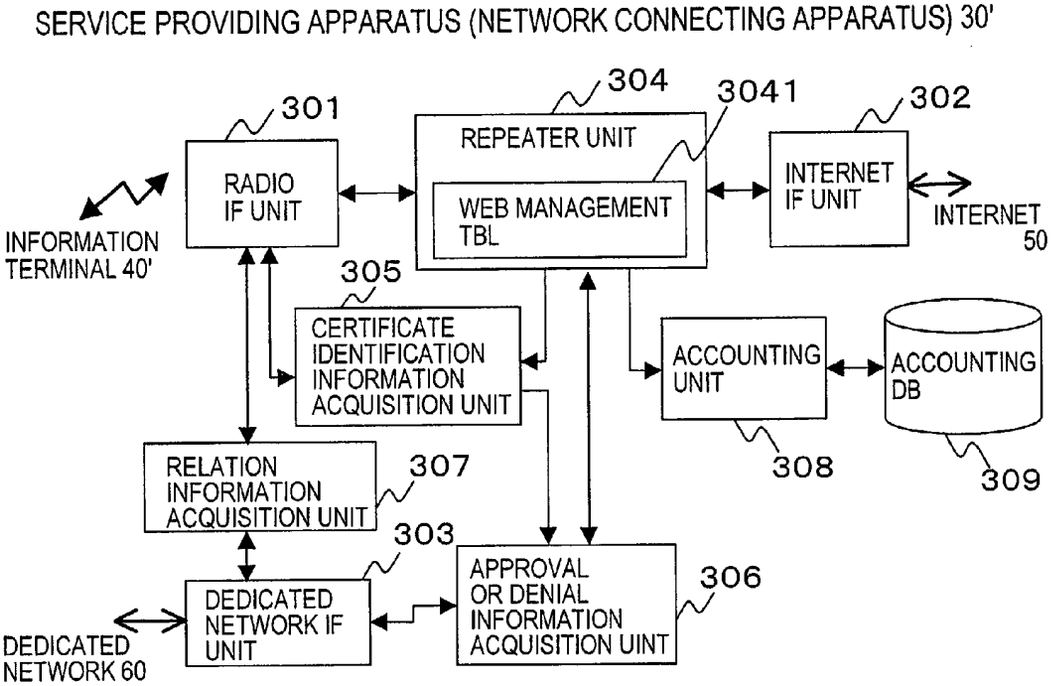


FIG.11

ACCOUNTING DB 309

3091 WEB PAGE IDENTIFICATION INFORMATION	3092 CERTIFICATE IDENTIFICATION INFORMATION	3093 USE FREQUENCY
******	****	** TIMES
	****	** TIMES
	⋮	⋮
******	****	** TIMES
	⋮	⋮
⋮	⋮	⋮

FIG.12

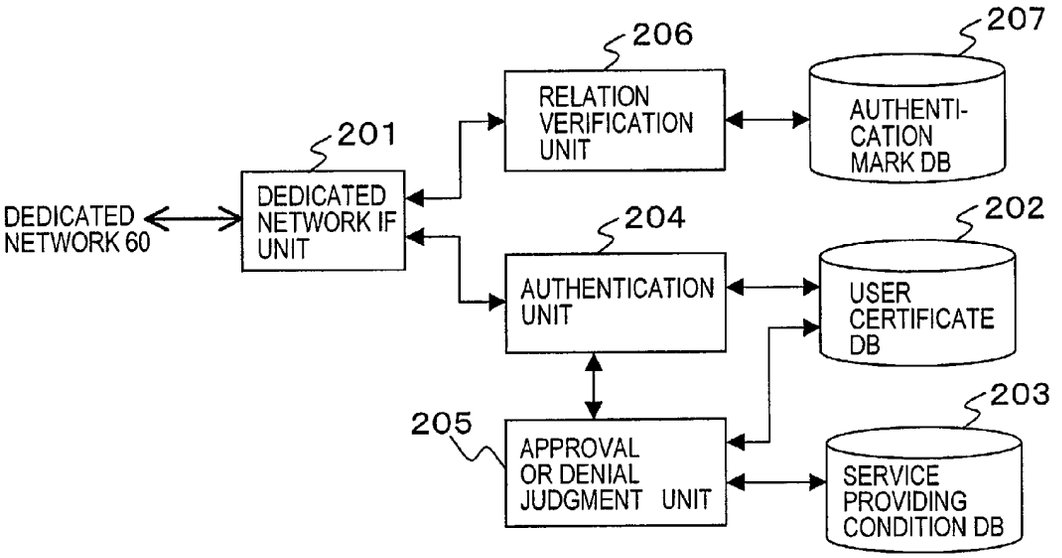


FIG.13

AUTHENTICATION MARK DB 207

2071 WEB PAGE IDENTIFICATION INFORMATION	2072 RELATED WEB PAGE IDENTIFICATION INFORMATION	2073 VERIFICATION KEY
****	****	****
⋮	⋮	⋮

FIG.14

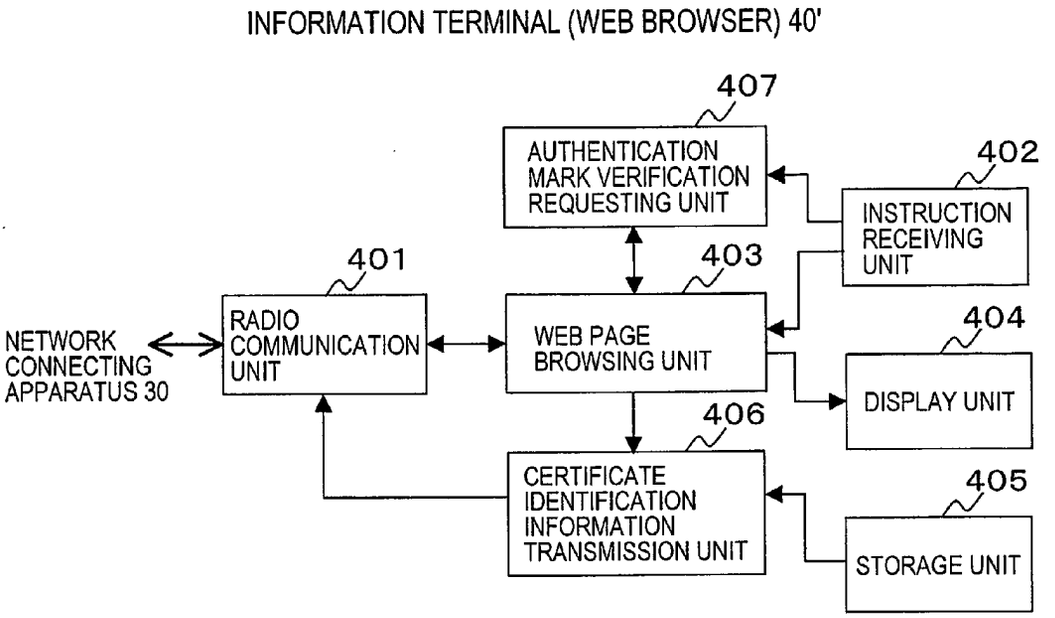

INFORMATION TERMINAL (WEB BROWSER) 40'
407
AUTHENTICATION MARK VERIFICATION REQUESTING UNIT
402
INSTRUCTION RECEIVING UNIT
401
403
NETWORK CONNECTING APPARATUS 30
RADIO COMMUNICATION UNIT
WEB PAGE BROWSING UNIT
404
DISPLAY UNIT
406
CERTIFICATE IDENTIFICATION INFORMATION TRANSMISSION UNIT
405
STORAGE UNIT

FIG.15

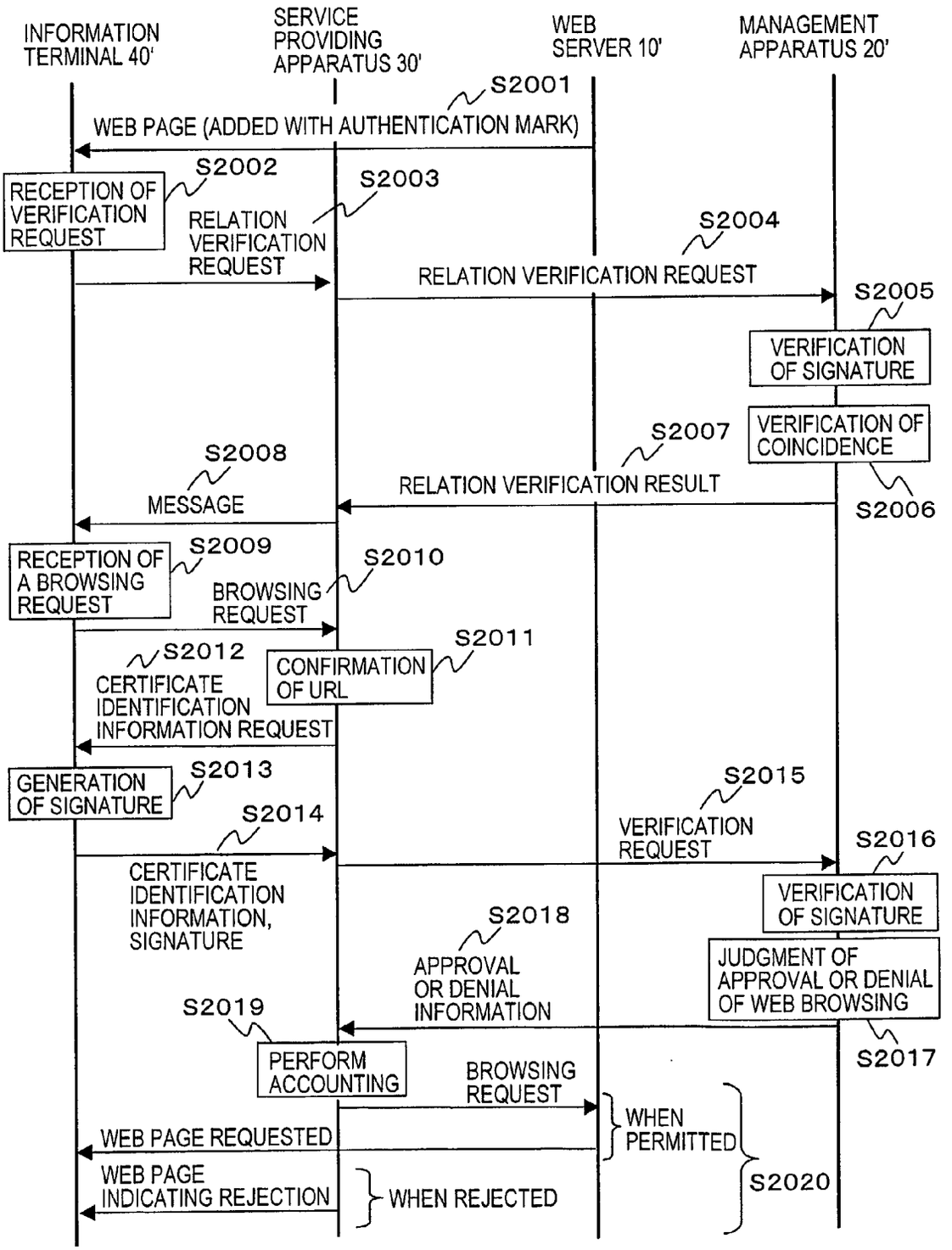

INFORMATION TERMINAL 40'
SERVICE PROVIDING APPARATUS 30'
WEB SERVER 10'
MANAGEMENT APPARATUS 20'
S2001
WEB PAGE (ADDED WITH AUTHENTICATION MARK)
S2002
RECEPTION OF VERIFICATION REQUEST
S2003
RELATION VERIFICATION REQUEST
S2004
RELATION VERIFICATION REQUEST
S2005
VERIFICATION OF SIGNATURE
VERIFICATION OF COINCIDENCE
S2006
S2007
RELATION VERIFICATION RESULT
S2008
MESSAGE
RECEPTION OF A BROWSING REQUEST
S2009
S2010
BROWSING REQUEST
S2011
CONFIRMATION OF URL
S2012
CERTIFICATE IDENTIFICATION INFORMATION REQUEST
GENERATION OF SIGNATURE
S2013
S2014
CERTIFICATE IDENTIFICATION INFORMATION, SIGNATURE
S2015
VERIFICATION REQUEST
S2016
VERIFICATION OF SIGNATURE
S2018
APPROVAL OR DENIAL INFORMATION
JUDGMENT OF APPROVAL OR DENIAL OF WEB BROWSING
S2017
S2019
PERFORM ACCOUNTING
BROWSING REQUEST
WHEN PERMITTED
WEB PAGE REQUESTED
WEB PAGE INDICATING REJECTION
WHEN REJECTED
S2020

FIG.16

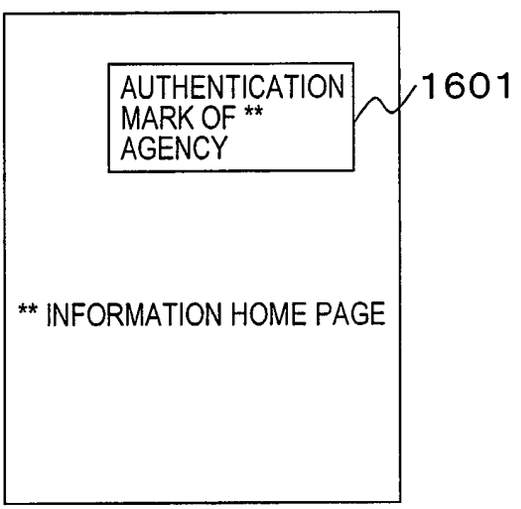


FIG.17

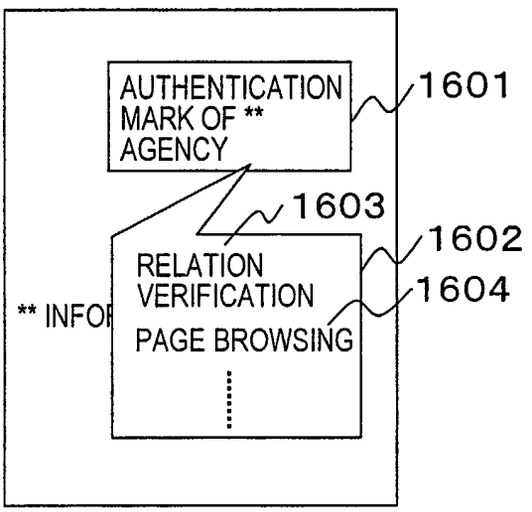

AUTHENTICATION MARK OF ** AGENCY
1601
1603
1602
RELATION VERIFICATION
1604
** INFOR
PAGE BROWSING

FIG.18

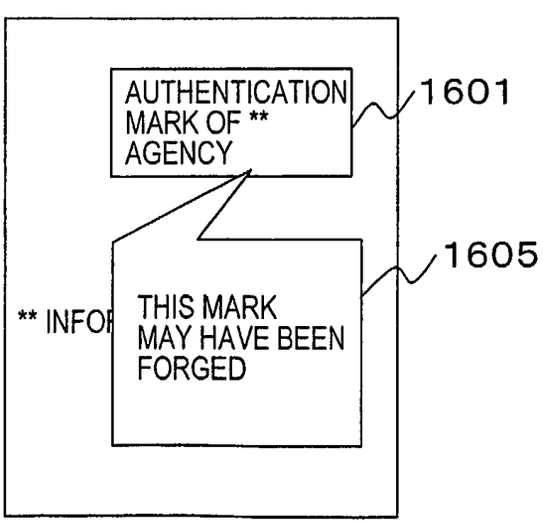

AUTHENTICATION MARK OF ** AGENCY
1601
1605
** INFOR
THIS MARK MAY HAVE BEEN FORGED

FIG.19

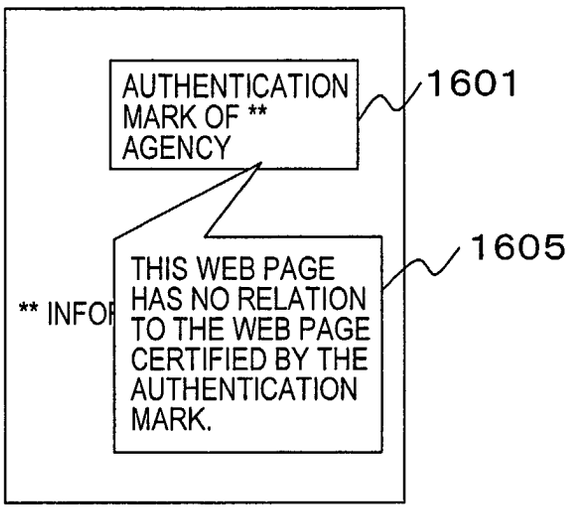

AUTHENTICATION MARK OF ** AGENCY
1601
1605
THIS WEB PAGE HAS NO RELATION TO THE WEB PAGE CERTIFIED BY THE AUTHENTICATION MARK.
** INFOR

FIG.20

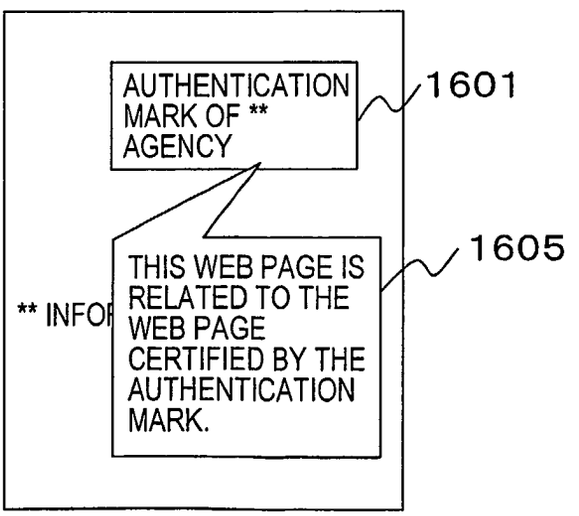

AUTHENTICATION MARK OF ** AGENCY
1601
1605
THIS WEB PAGE IS RELATED TO THE WEB PAGE CERTIFIED BY THE AUTHENTICATION MARK.
** INFOR

FIG.21

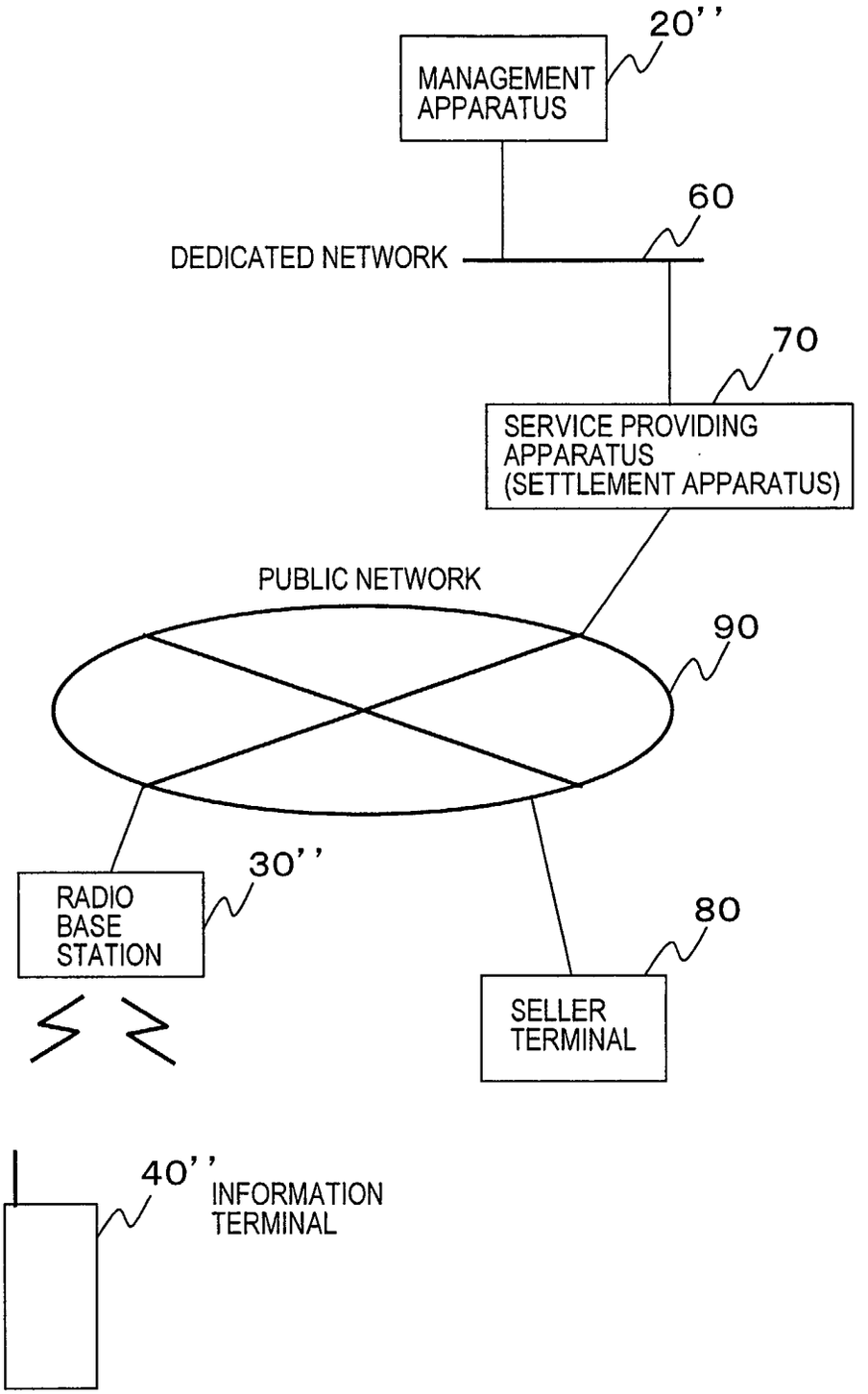

20''
MANAGEMENT APPARATUS
60
DEDICATED NETWORK
70
SERVICE PROVIDING APPARATUS (SETTLEMENT APPARATUS)
PUBLIC NETWORK
90
30''
RADIO BASE STATION
80
SELLER TERMINAL
40''
INFORMATION TERMINAL

FIG.22

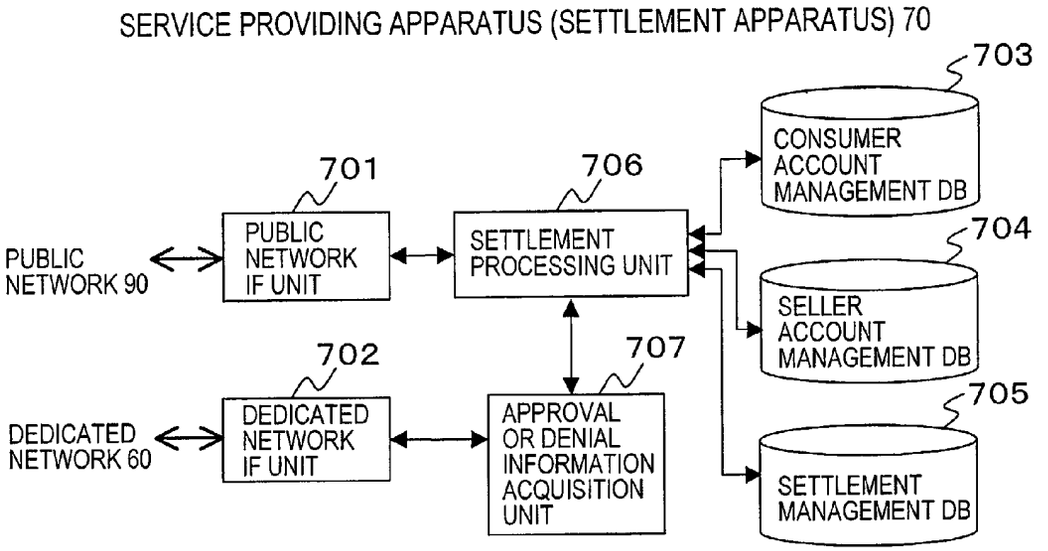


FIG.23

SETTLEMENT MANAGEMENT DB 705

7051 MANAGEMENT NUMBER	7052 SELLER'S SIDE SETTLEMENT REQUEST	7053 CONSUMER'S SIDE SETTLEMENT REQUEST	7054 SETTLEMENT STATE
******	******	******	SETTLED
******	******	******	SETTLED
******	******		UNSETTLED
******	******	*****	FAILURE
⋮	⋮	⋮	⋮

FIG.24

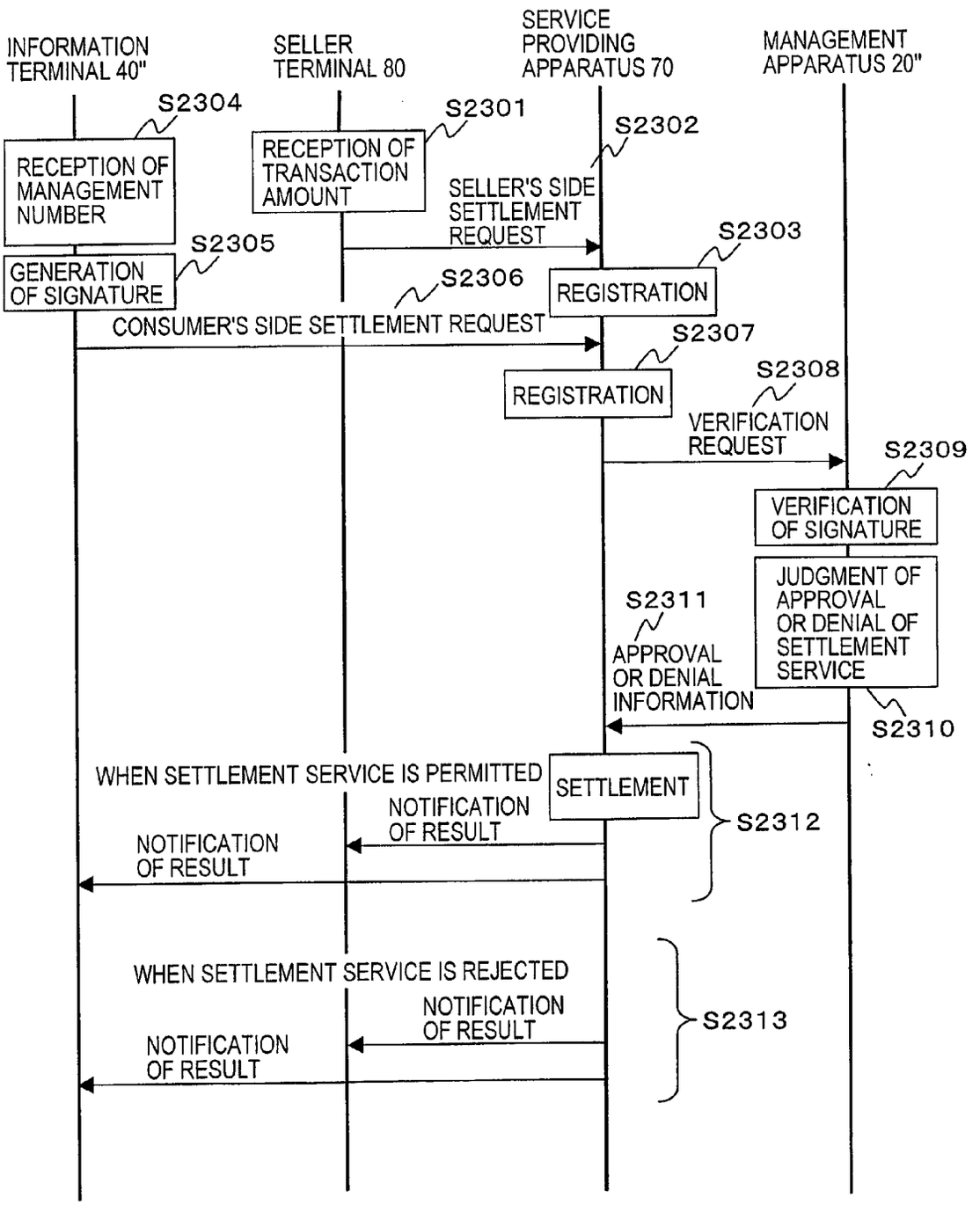
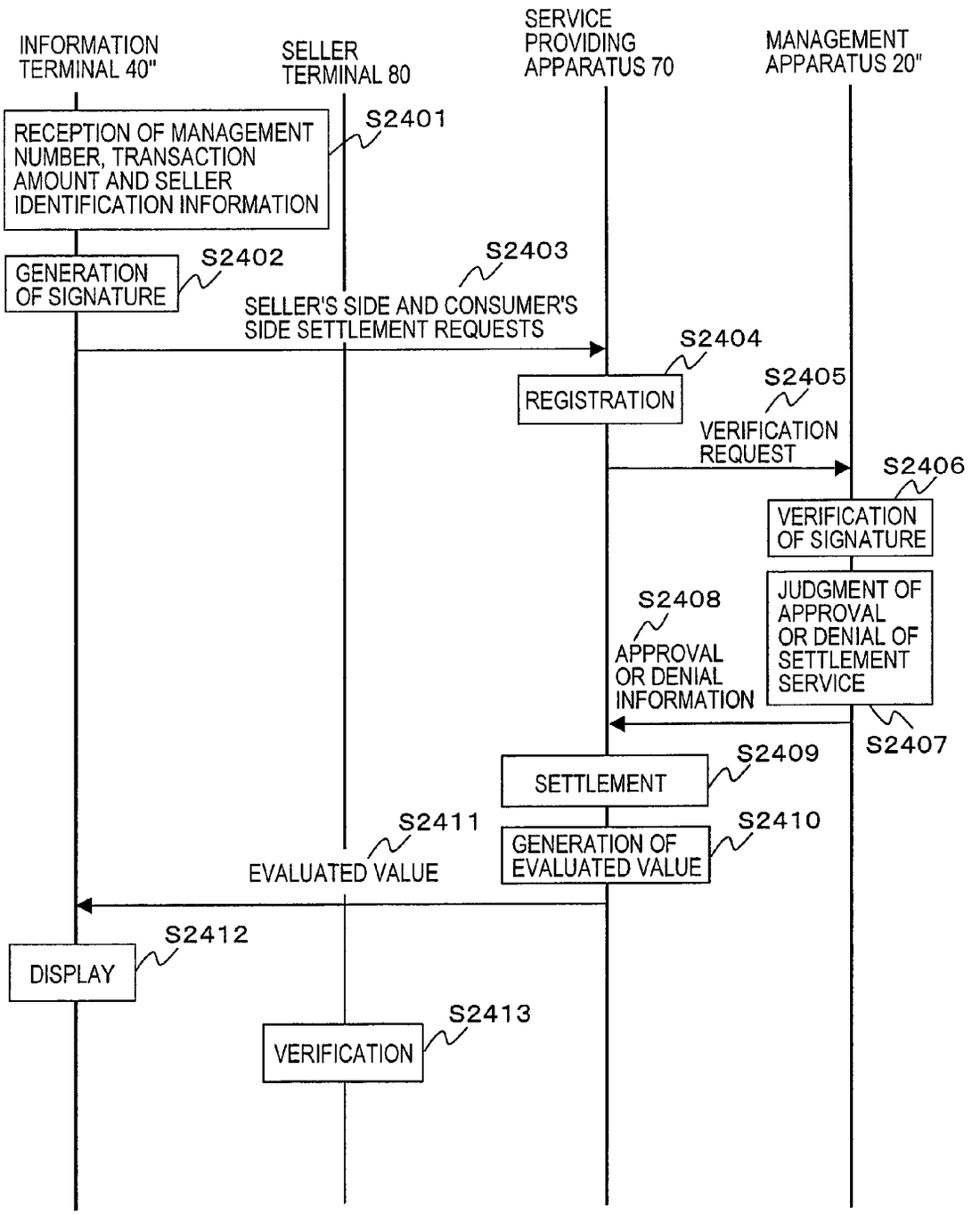

INFORMATION TERMINAL 40"
SELLER TERMINAL 80
SERVICE PROVIDING APPARATUS 70
MANAGEMENT APPARATUS 20"
S2304
RECEPTION OF MANAGEMENT NUMBER
S2301
RECEPTION OF TRANSACTION AMOUNT
S2302
SELLER'S SIDE SETTLEMENT REQUEST
S2303
REGISTRATION
S2305
GENERATION OF SIGNATURE
S2306
CONSUMER'S SIDE SETTLEMENT REQUEST
S2307
REGISTRATION
S2308
VERIFICATION REQUEST
S2309
VERIFICATION OF SIGNATURE
JUDGMENT OF APPROVAL OR DENIAL OF SETTLEMENT SERVICE
S2311
APPROVAL OR DENIAL INFORMATION
S2310
WHEN SETTLEMENT SERVICE IS PERMITTED
SETTLEMENT
NOTIFICATION OF RESULT
NOTIFICATION OF RESULT
S2312
WHEN SETTLEMENT SERVICE IS REJECTED
NOTIFICATION OF RESULT
NOTIFICATION OF RESULT
S2313

FIG.25


INFORMATION TERMINAL 40"
SELLER TERMINAL 80
SERVICE PROVIDING APPARATUS 70
MANAGEMENT APPARATUS 20"
RECEPTION OF MANAGEMENT NUMBER, TRANSACTION AMOUNT AND SELLER IDENTIFICATION INFORMATION
S2401
GENERATION OF SIGNATURE
S2402
S2403
SELLER'S SIDE AND CONSUMER'S SIDE SETTLEMENT REQUESTS
S2404
REGISTRATION
S2405
VERIFICATION REQUEST
S2406
VERIFICATION OF SIGNATURE
JUDGMENT OF APPROVAL OR DENIAL OF SETTLEMENT SERVICE
S2407
S2408
APPROVAL OR DENIAL INFORMATION
S2409
SETTLEMENT
S2410
GENERATION OF EVALUATED VALUE
S2411
EVALUATED VALUE
S2412
DISPLAY
S2413
VERIFICATION